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

First, I downloaded John the Ripper, a password cracking tool, and installed it on my computer. I followed the instructions carefully, as I did not want to accidentally damage my system. After the program was installed, I opened it and started exploring its features.

At first, I was a bit intimidated by the command-line interface and the various options available. However, after reading through online tutorials and experimenting with the program, I began to understand how it worked. Essentially, John the Ripper uses various techniques to guess or brute-force passwords, such as dictionary attacks and rainbow tables.

To test the program, I used a password-protected ZIP file that I had created. I ran John the Ripper against the file and watched as it tried different combinations of characters to crack the password. It took a few minutes, but eventually, the program was able to guess the password and unlock the file.

Next, I turned my attention to Spyrix, a keylogger. I had read that keyloggers were often used by hackers to capture sensitive information, such as passwords and credit card numbers. I downloaded and installed Spyrix on my computer, again following the instructions carefully.

Once the program was installed, I started it up and began exploring its features. Spyrix worked quietly in the background, capturing keystrokes and taking screenshots at regular intervals. I was able to view this information in real-time from a remote location, which was both fascinating and a little unnerving.

Overall, my experience using John the Ripper and Spyrix was an enlightening one. These tools gave me a better understanding of how cybersecurity professionals test the strength of their systems and how malicious actors may try to gain unauthorized access to sensitive information.

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

My findings showed that John the Ripper was an effective password cracking tool that could be used by cybersecurity professionals to test the strength of their systems. However, it was also apparent that the program could be used by malicious actors to gain unauthorized access to sensitive information. As for Spyrix, the keylogger was a powerful tool that could capture keystrokes and screenshots, giving someone access to sensitive information.

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

Through my research, I learned that cybersecurity is a complex and constantly evolving field. I also learned that while tools like John the Ripper and Spyrix could be used for good purposes, they could also be used by malicious actors to gain unauthorized access to sensitive information. This was a sobering reminder of the importance of staying vigilant and keeping our systems secure. Additionally, I gained a better understanding of how password cracking and keylogging tools work and how they interact with a computer.