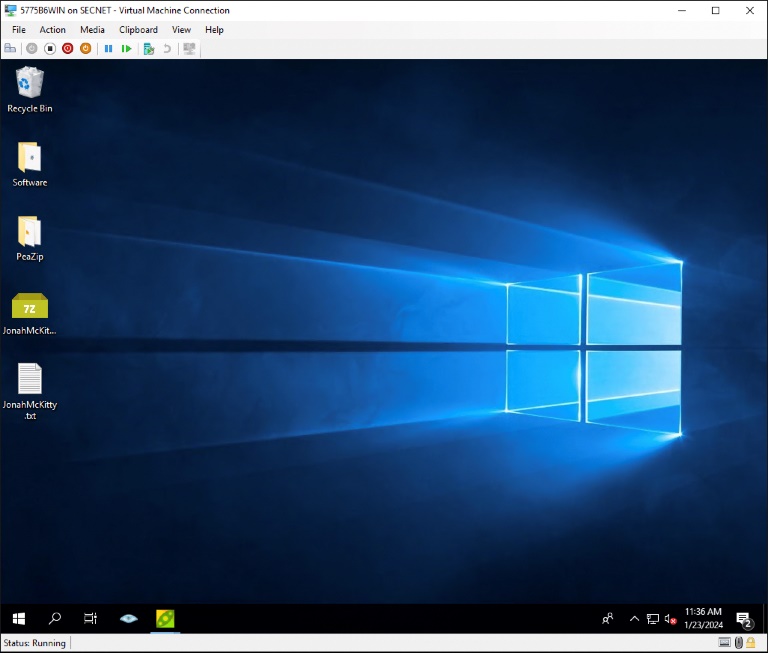
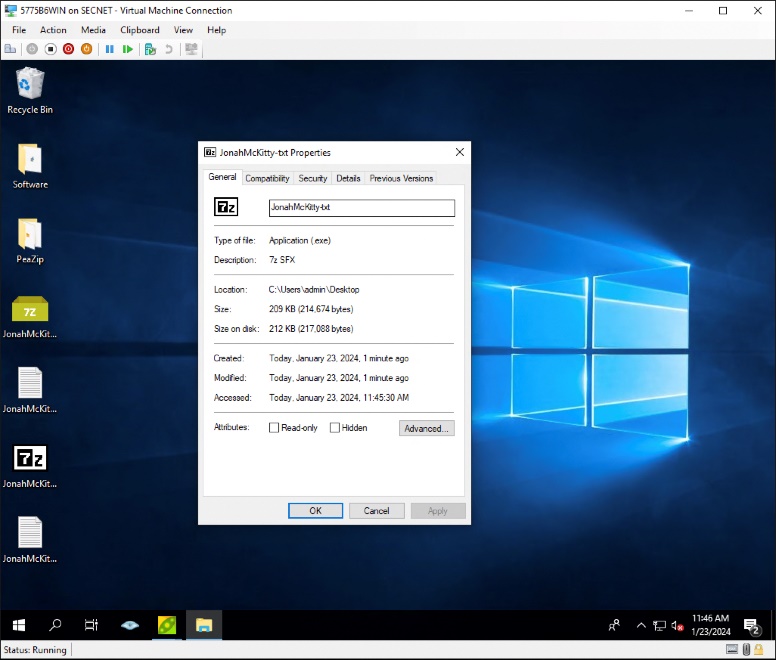
Jonah McKitty

LIS5775

Lab 2



2 .exe file created from .txt file

1.txt file created

1. Why would you need an encrypted file that self-extracts (.exe)?

The use of an encrypted self-extracting (.exe) file can be beneficial for securely sharing sensitive information. This type of file allows the recipient to extract the contents without needing a separate extraction tool while maintaining the encryption for security during transit.

1. Will PeaZip or AxCrypt work on multiple files or entire directories (folders)?

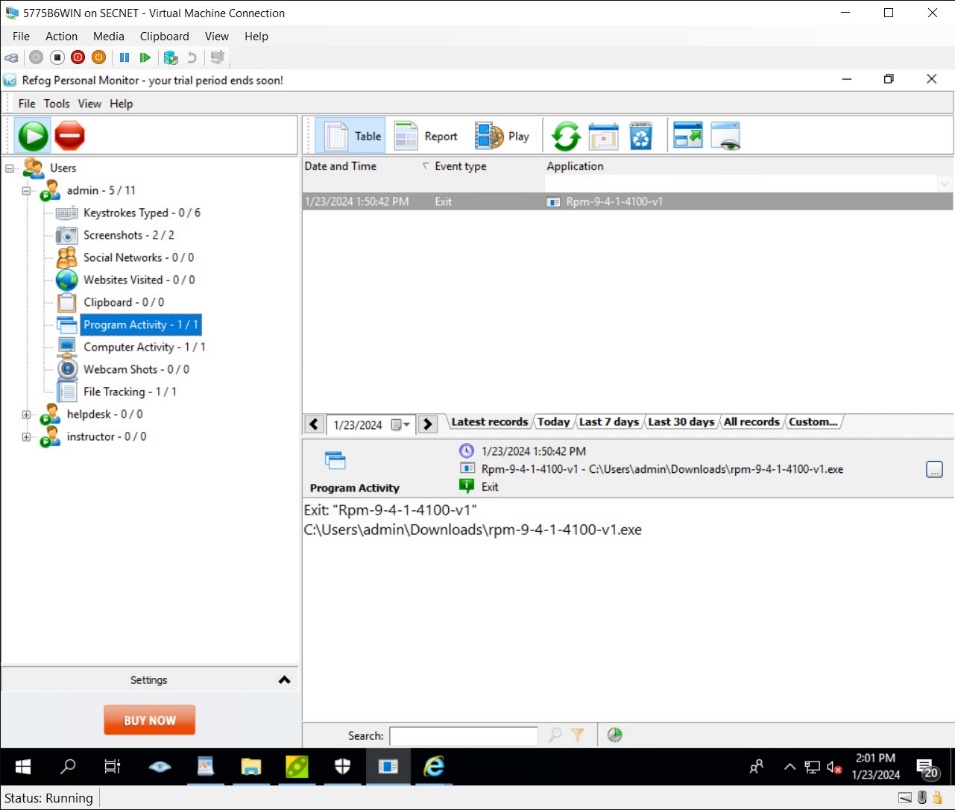
Yes, You can use PeaZip for compressing and extracting multiple files or entire directories

1. Even if you encrypted a file with PeaZip or AxCrypt, wouldn’t someone be able to recover a previous version of the file with a file recovery program? Hint: AxCrypt has a built-in shredder.

When you encrypt a file using tools like PeaZip or AxCrypt, it typically involves overwriting the original file with the encrypted version. This process makes it challenging for file recovery programs to retrieve previous versions since the original data is effectively replaced. AxCrypt's built-in shredder further enhances security by securely deleting the original unencrypted data.

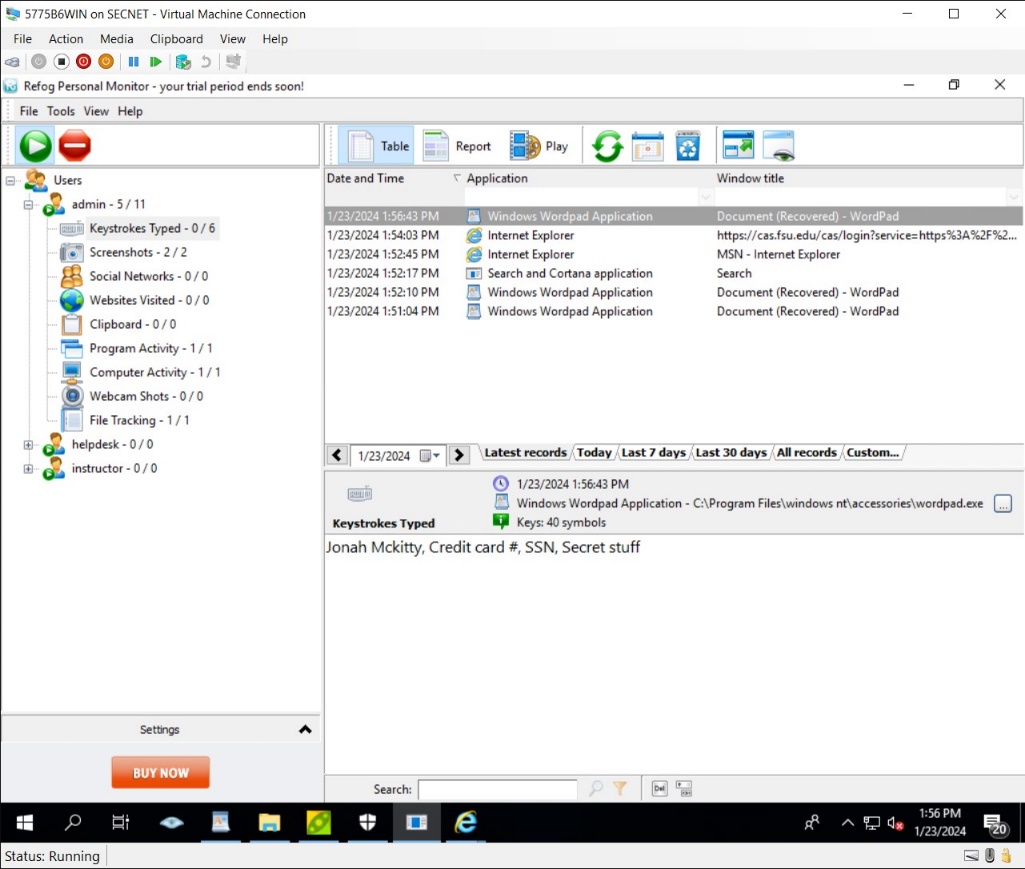
1. Could your network administrator open these files after you encrypted them with PeaZip or AxCrypt? Why not?

Encryption tools use strong encryption algorithms to protect files, and only individuals with the correct decryption key (passphrase or password) can access the content. Network administrators may have access to network traffic but should not be able to decrypt and open files encrypted with proper security measures.

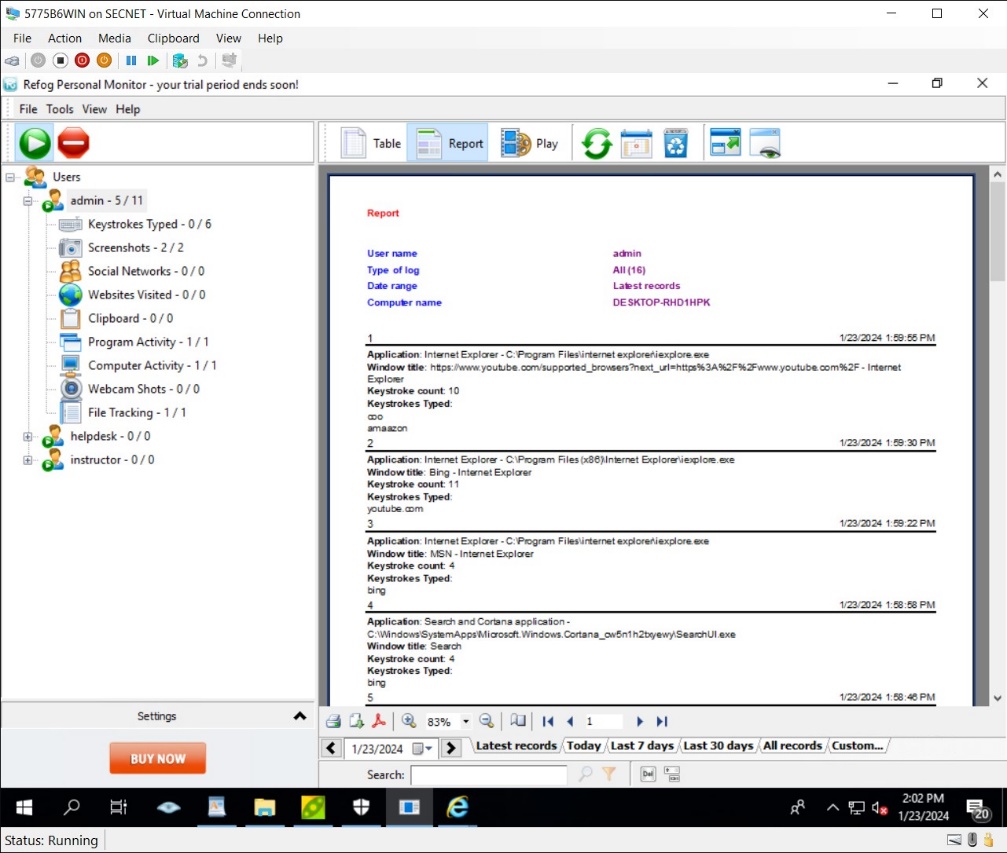
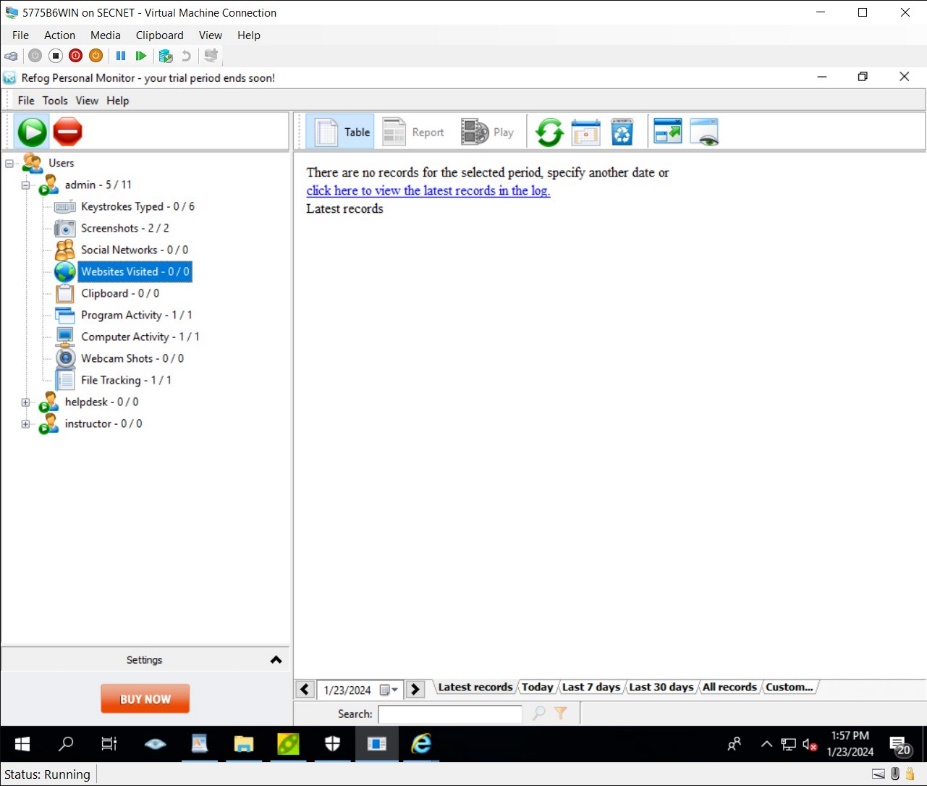


1. Program Activity

2 Websites Visited



2. Keystrokes Typed



3. Websites Visited \*\*Refog struggled to log the sites I visited, you can view those in the Keystrokes Typed picture

4. Report from Refog

1. Does your employer / spouse / roommate monitor your activities with a keylogger? Are you sure?

My employer does not monitor my activites with a keylogger. I am very sure because I work as an IT Technician, I have knowledge of all the programs that are installed on our machines during the building process.

1. What would happen if your employer / spouse / roommate finds out you were using a keylogger to monitor their activities?

I am pretty sure that they would not be too happy with me and may even pursue legal action against me depending on how they found out.

1. Why would someone want to install a keylogger on their own computer?

I don’t think there are many scenarios where someone would want to install a keylogger on their own computer but perhaps if they wanted to monitor their own computer activities or keep track of passwords in case of forgetfulness.

1. How would you know if you had a keylogger on your computer? How would you get rid of it?

Keyloggers operate very discreetly however, some signs may include unusual system behavior, unexpected slowdowns, or suspicious network activity. To get rid of it, I would run a full system scan using up-to-date anti-malware or antivirus software. Update my operating system and all installed applications to patch any security vulnerabilities and use a dedicated anti-keylogger tool to specifically target and remove keyloggers.