Student:	Email:
Jacob Jeffers	jjeffers6151@ucumberlands.edu

Time on Task:	Progress:
5 hours, 45 minutes	100%

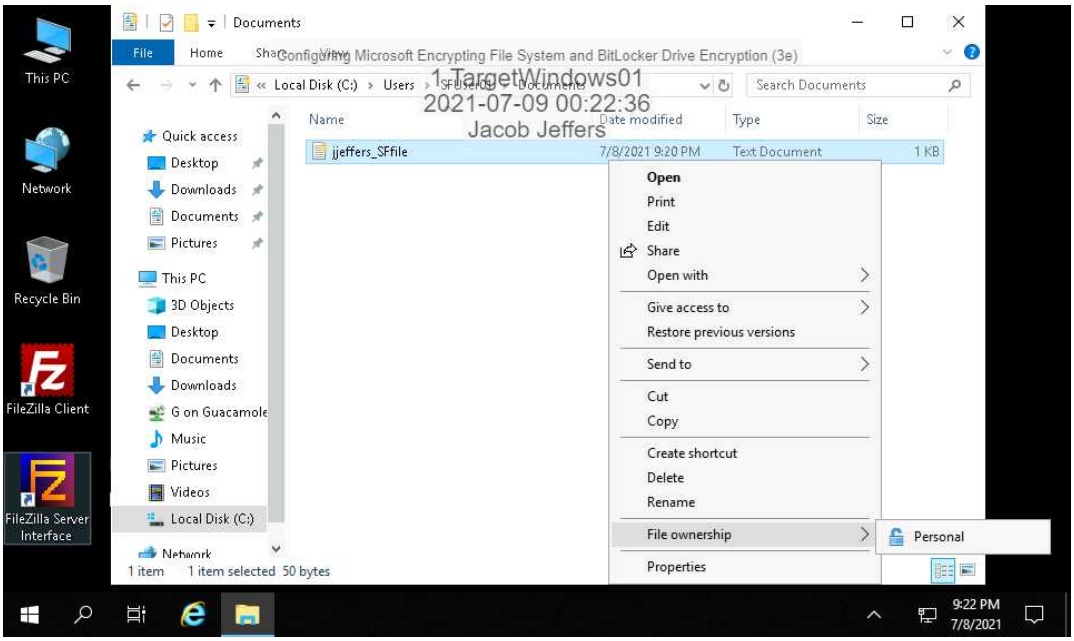
Report Generated: Friday, July 9, 2021 at 1:22 AM

Section 1: Hands-On Demonstration

Part 1: Configure Microsoft Encrypted File System (EFS)

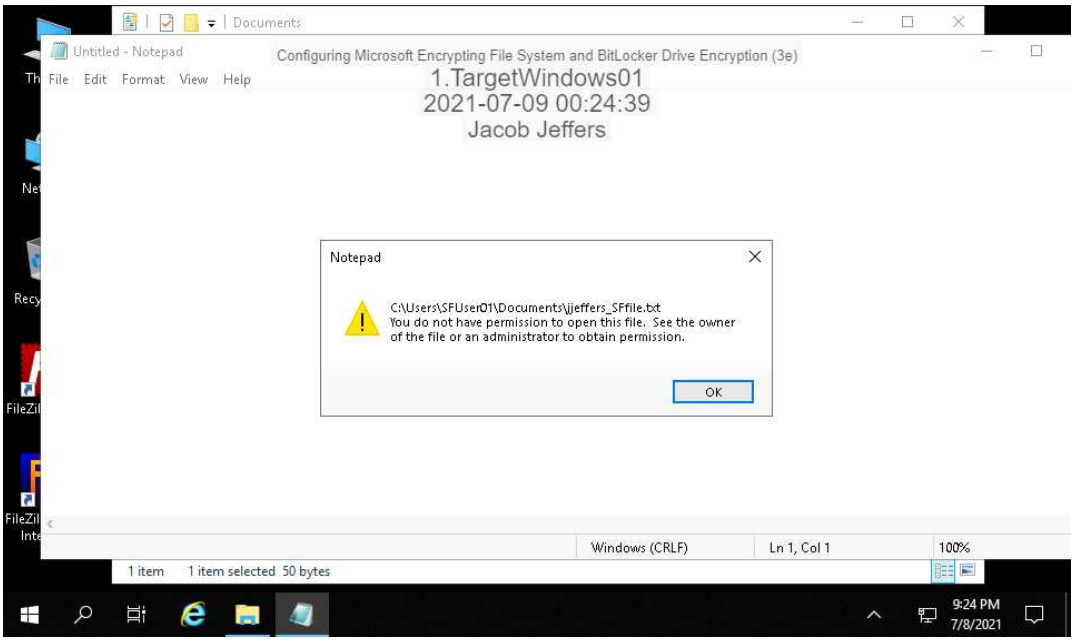
17. **Make a screen capture** showing the **encrypted Documents folder**.

    The Documents folder now includes a lock icon indicating that the folder and its contents are now encrypted.



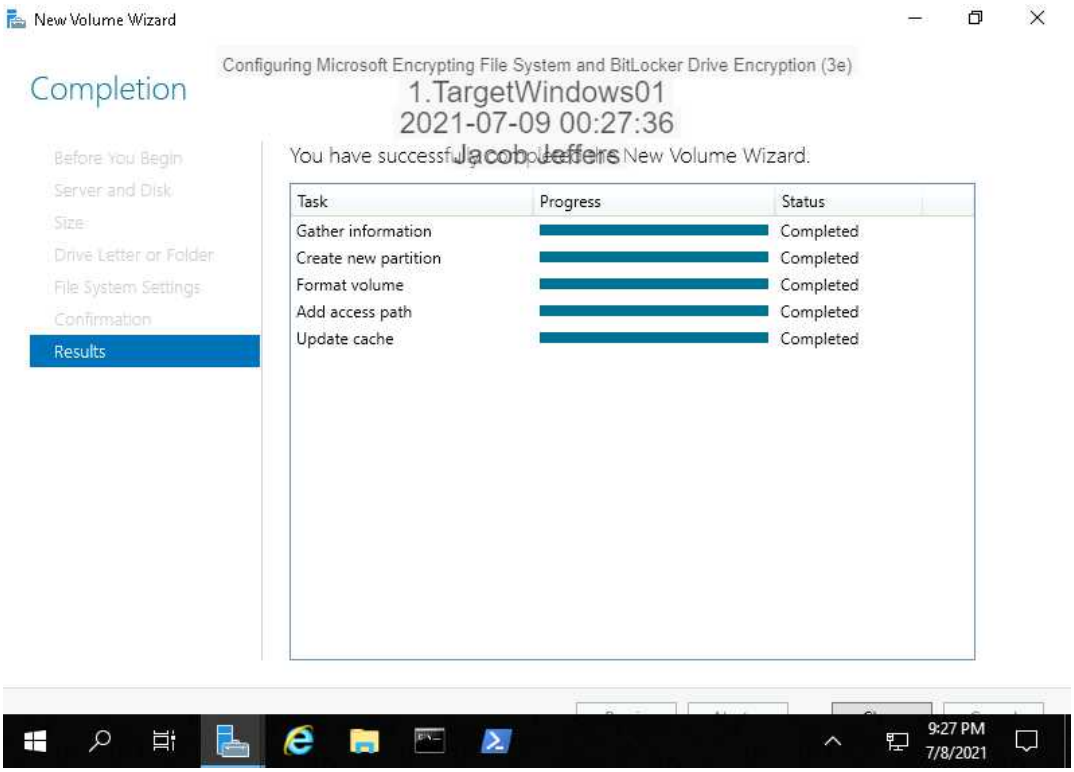
Part 2: Test the EFS Security

6. **Make a screen capture** showing **Notepad and the alert message**.

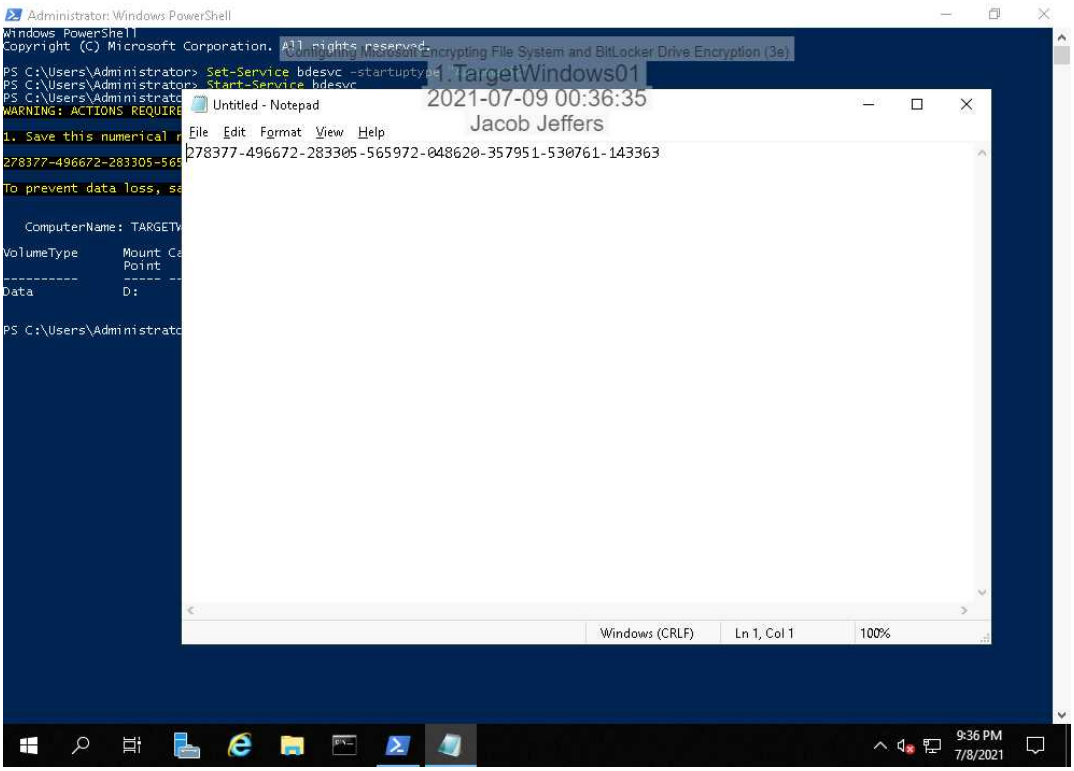


Part 3: Configure BitLocker

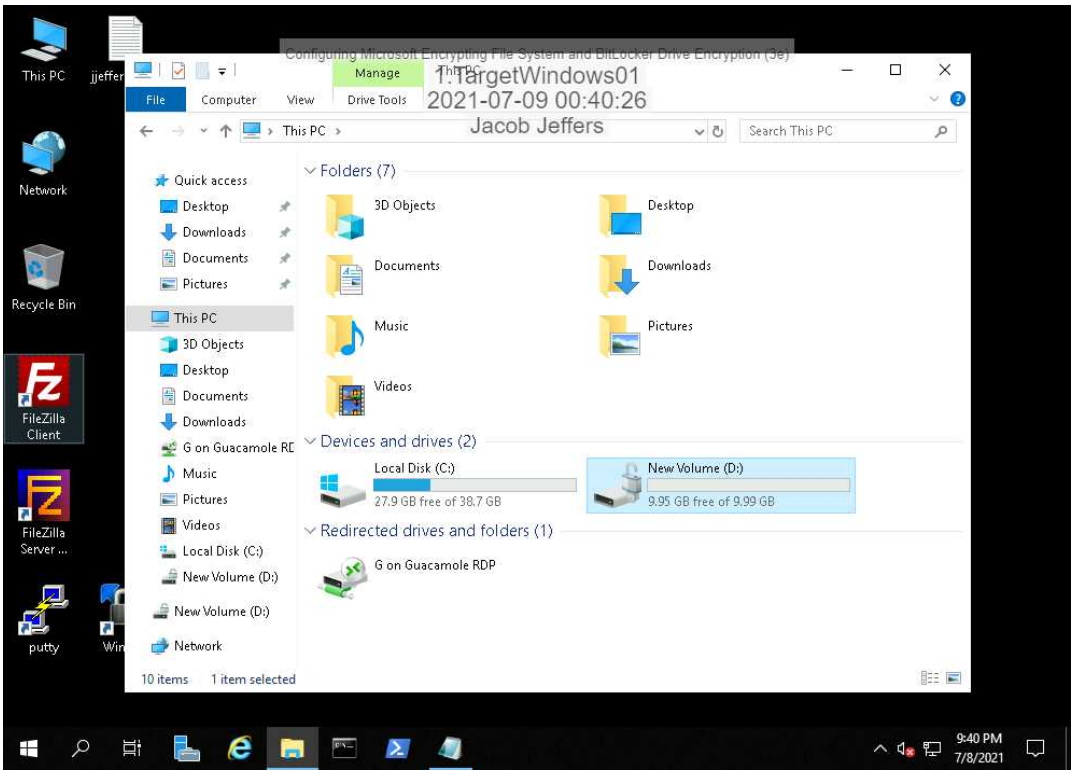
11. **Make a screen capture** showing the **settings on the Confirmation page**.



26. **Make a screen capture** showing **Notepad and the BitLocker recovery key**.



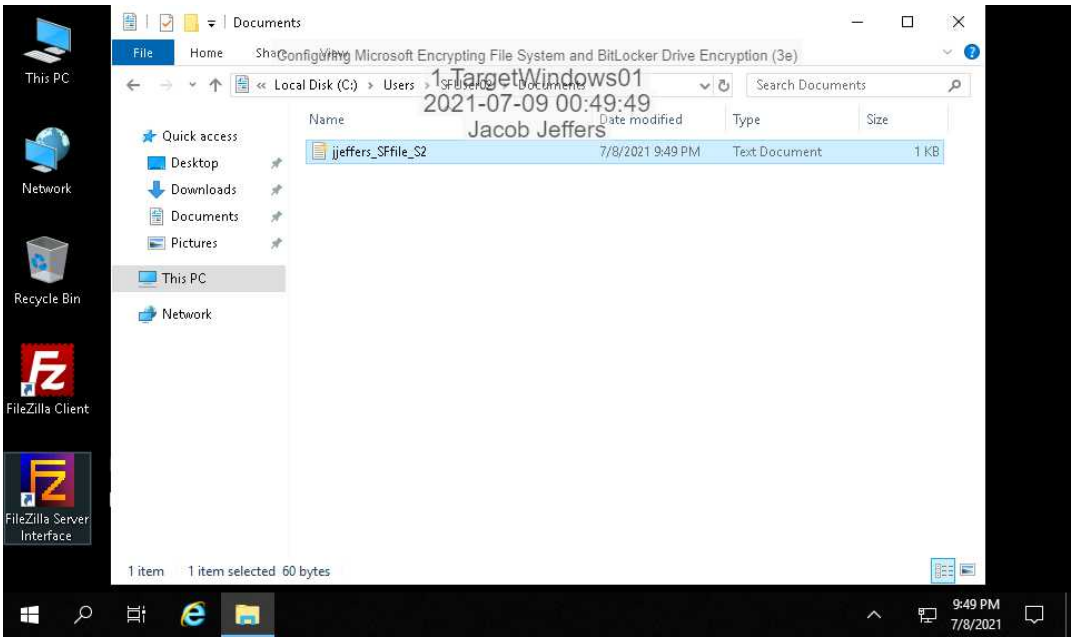
40. **Make a screen capture** showing the **This PC view with the unlocked drive**.



Section 2: Applied Learning

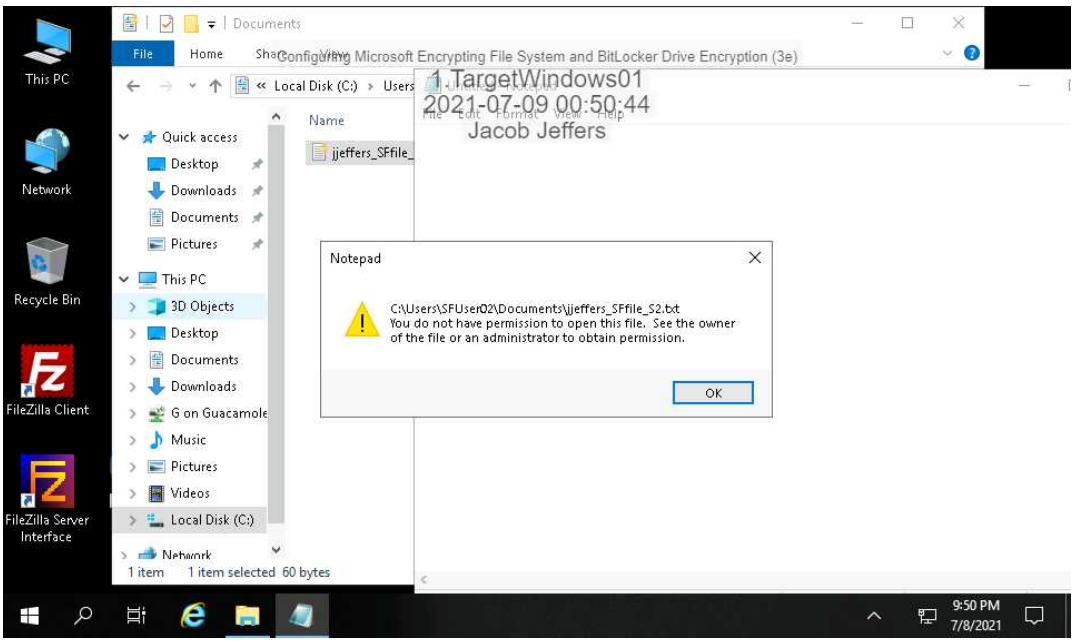
Part 1: Configure Microsoft Encrypted File System (EFS)

6. **Make a screen capture** showing the **encrypted SFUser02 Documents folder**.



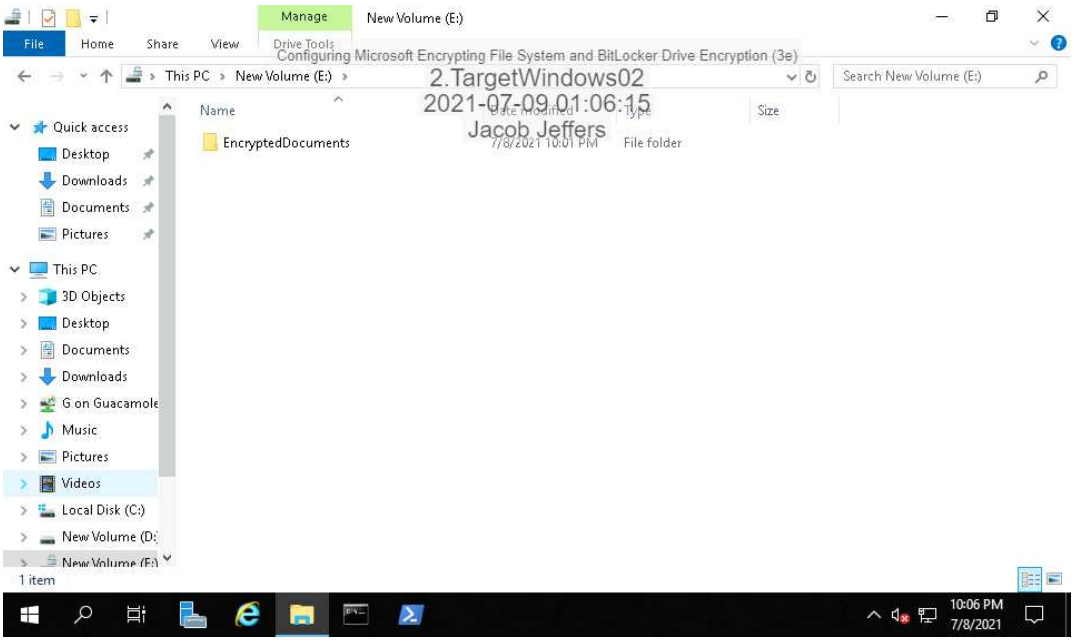
Part 2: Test the EFS Security

4. **Make a screen capture** showing **Notepad and the error message**.

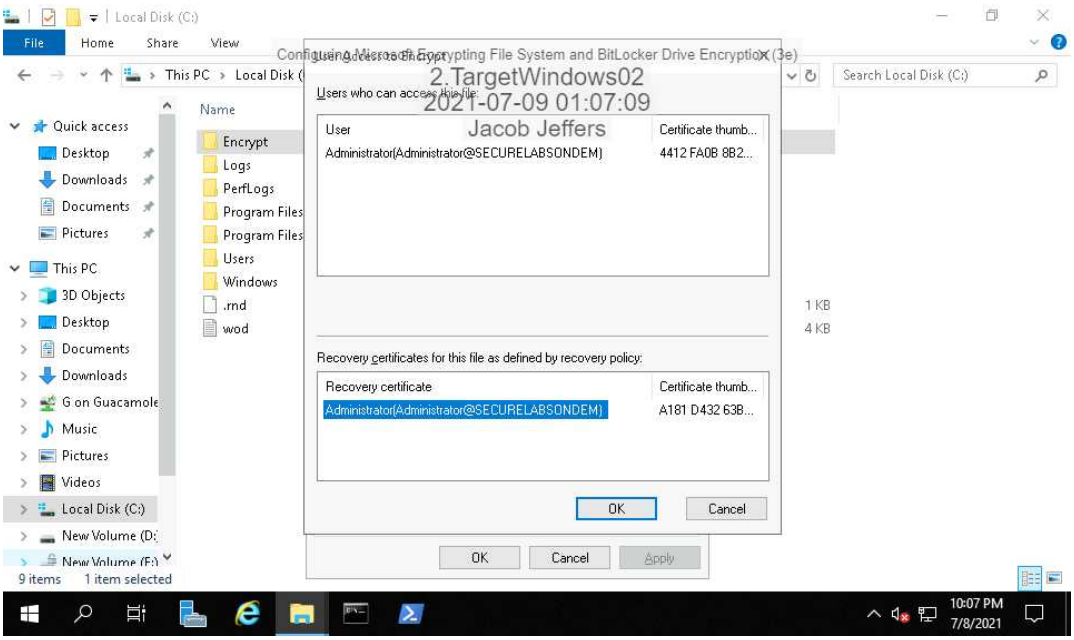


Part 3: Configure BitLocker

28. **Make a screen capture** showing the **unlocked E: drive in the File Explorer**.



31. **Make a screen capture** showing the **User Access details for the Encrypt folder**.



Section 3: Challenge and Analysis

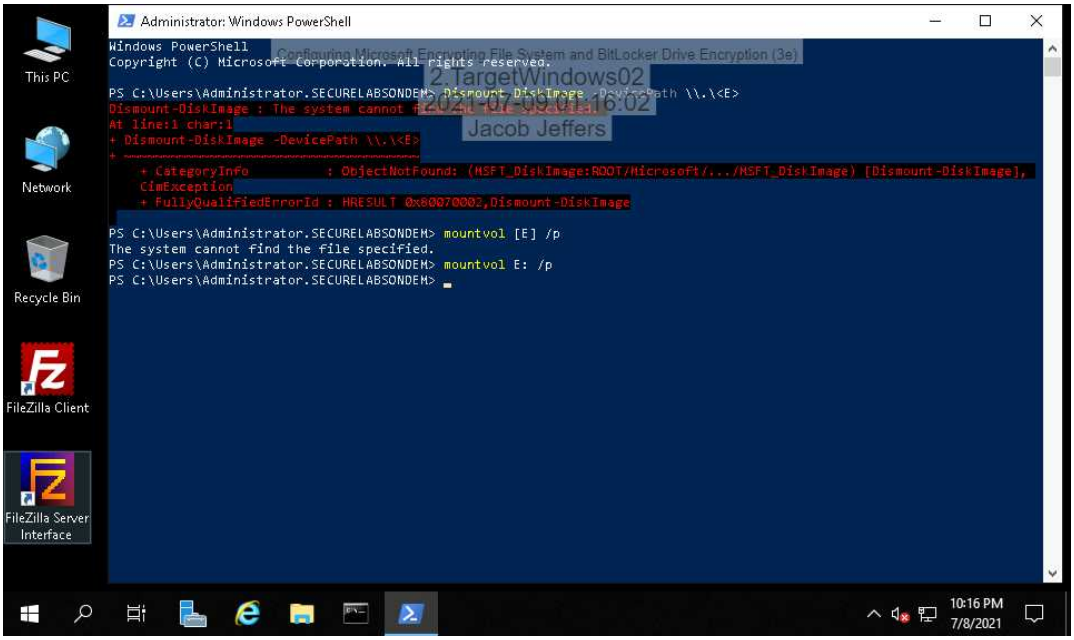
Part 1: Analysis and Discussion

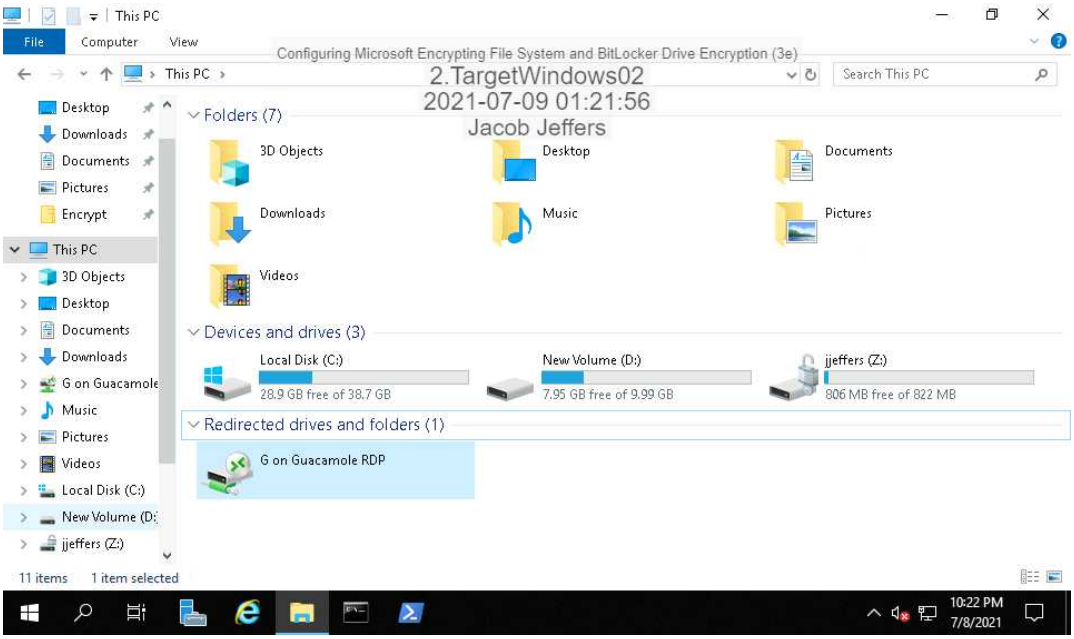
In the lab, you learned that Microsoft's BitLocker encryption utility can be defeated by another Microsoft program: COFEE (Computer Online Forensic Evidence Extractor). What is your opinion about Microsoft's strategy of releasing a program that can crack its own encryption utility?

I actually did some research into this, and COFEE was developed by a former cop who worked in Hong Kong. The solution was to plug in a USB device and let the contents on that drive unencrypt the encrypted drive. It was initially released as a tool for computer forensic investigators. Personally, my opinion is that it is a violation of privacy.

Part 2: Tools and Commands

Make a screen capture showing the **PowerShell command(s) used to unmount the E: drive**.



Part 3: Challenge Exercise

Make a screen capture showing the **encrypted *yourname* Z: drive**.