Student:	Email:
Bradley Adams	badams10@my.athens.edu

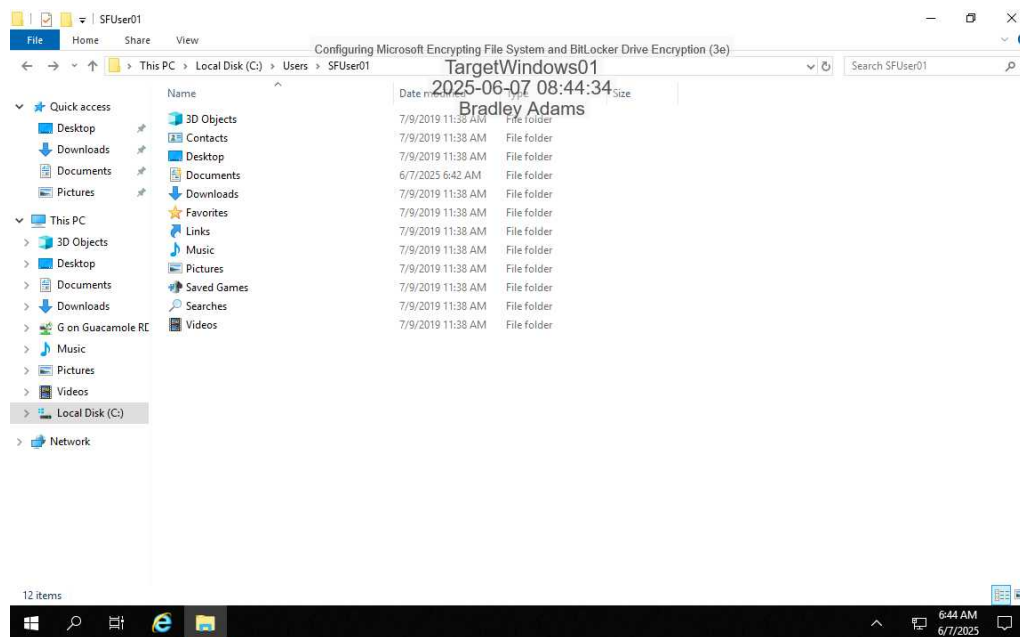| Time on Task:	Progress:
8 hours, 42 minutes	100%

Report Generated: Saturday, June 7, 2025 at 12:24 PM

Section 1: Hands-On Demonstration

Part 1: Configure Microsoft Encrypted File System (EFS)
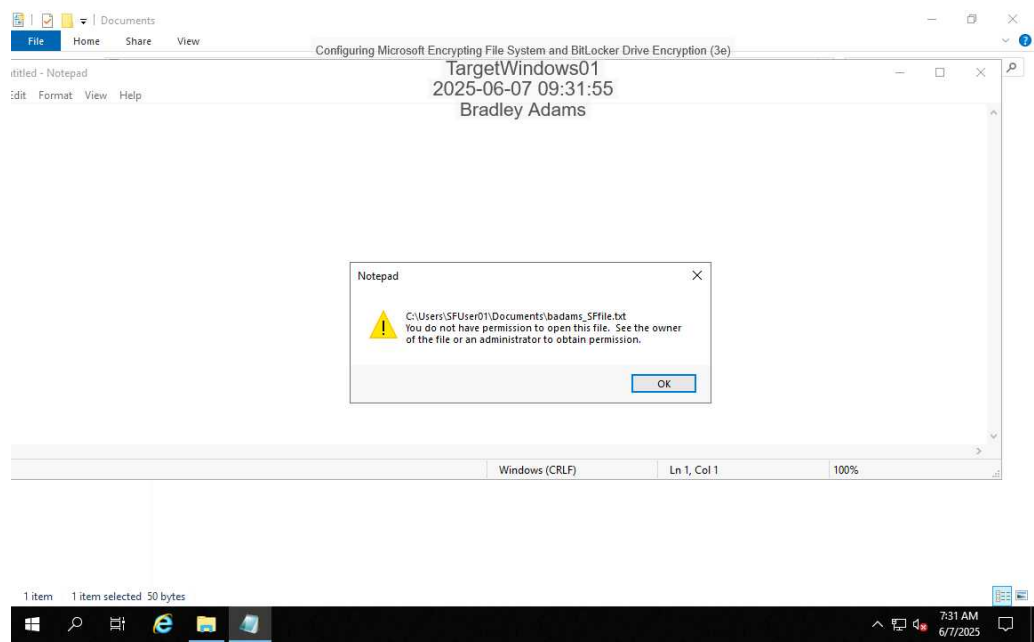
17. **Make a screen capture** showing the **encrypted Documents folder**.

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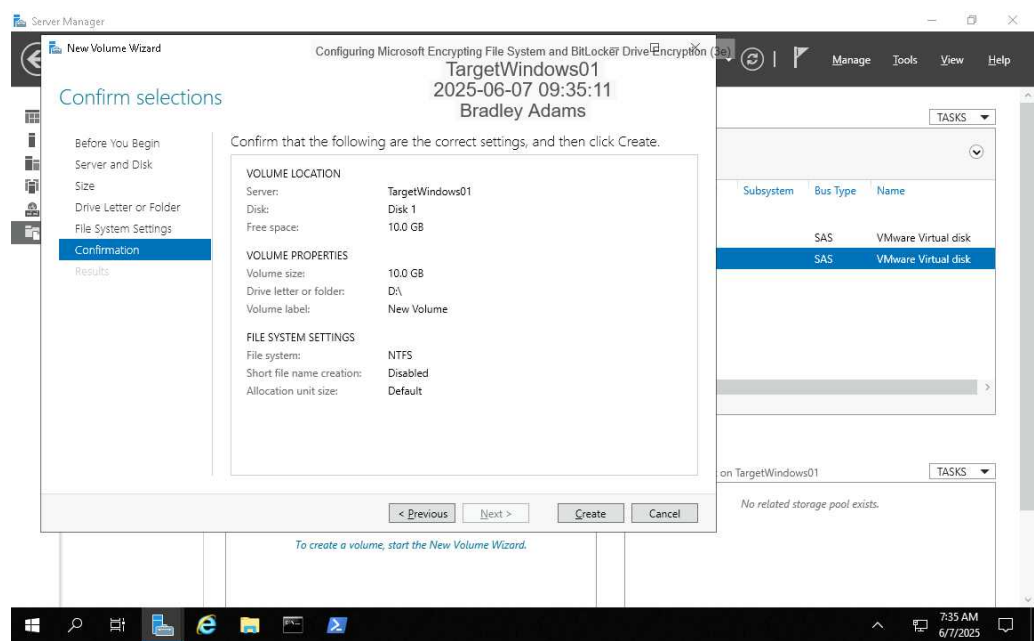

Part 2: Test the EFS Security

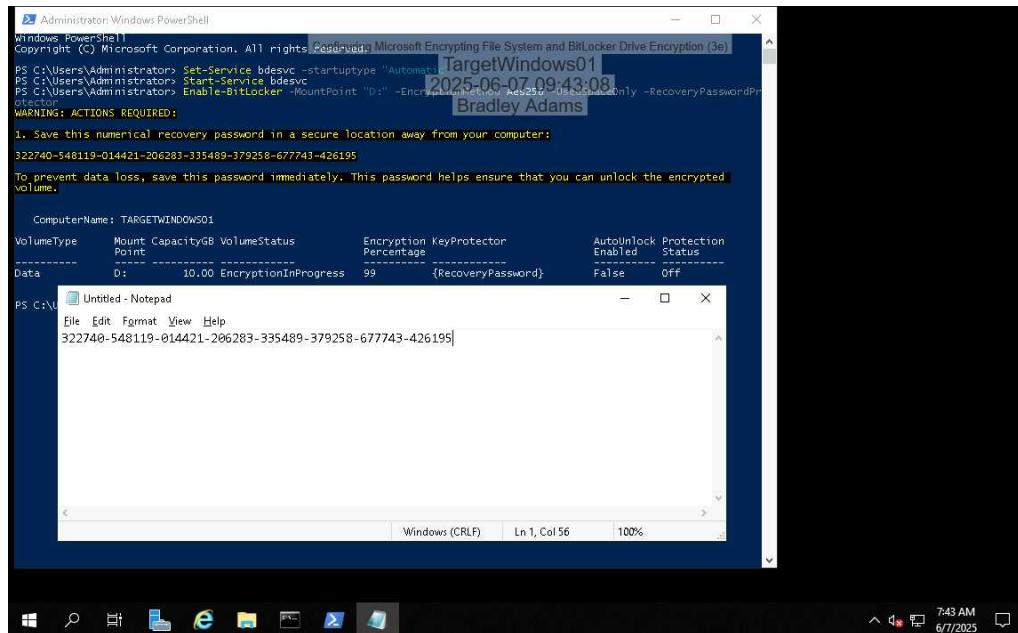6. **Make a screen capture** showing **Notepad and the alert message**.
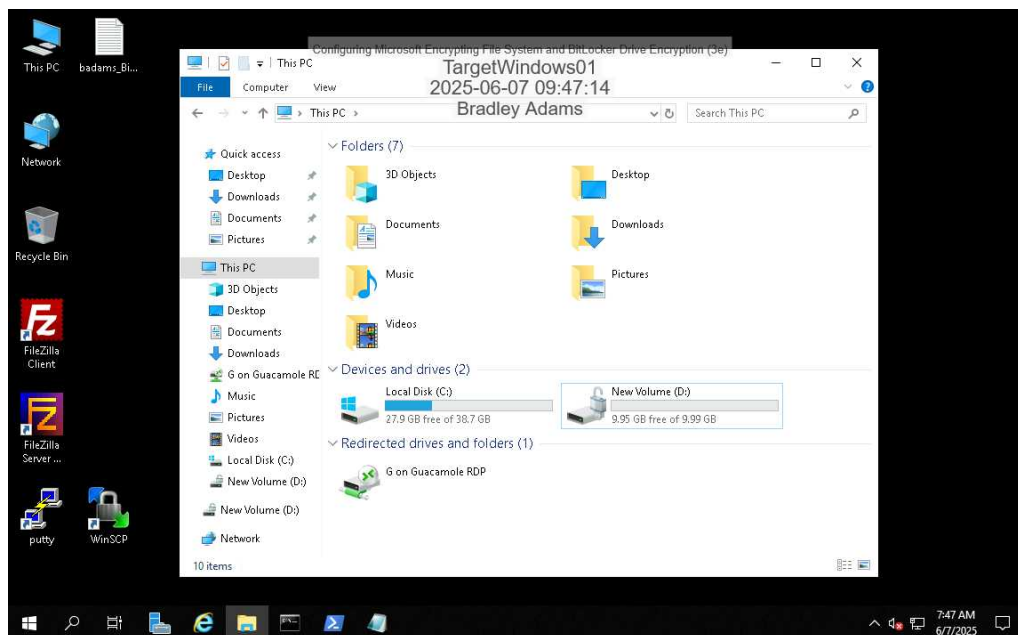

Part 3: Configure BitLocker

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

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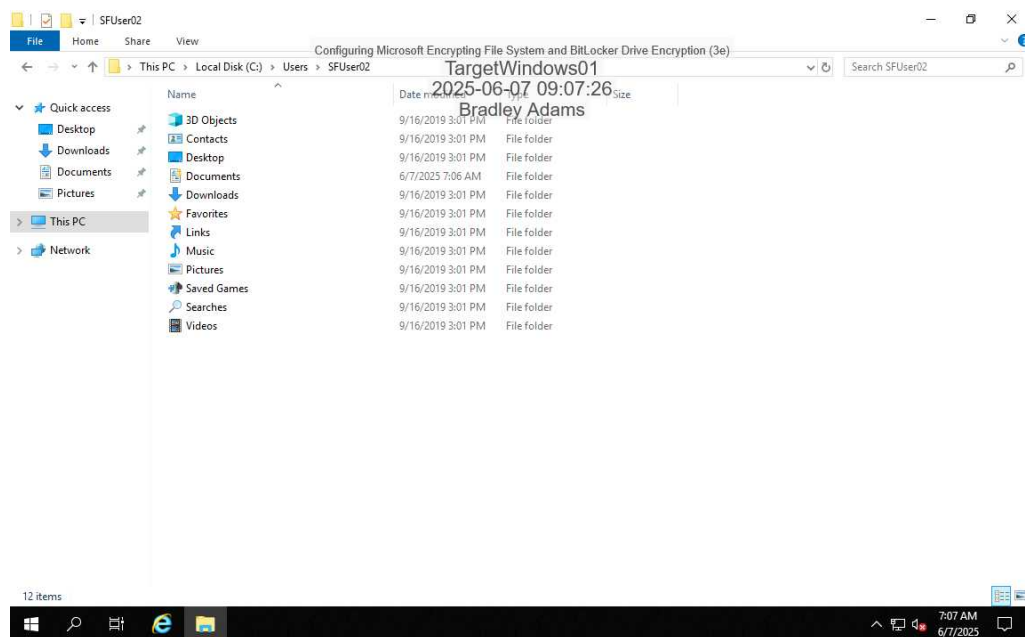

40. **Make a screen capture** showing the **This PC view with the unlocked drive**.

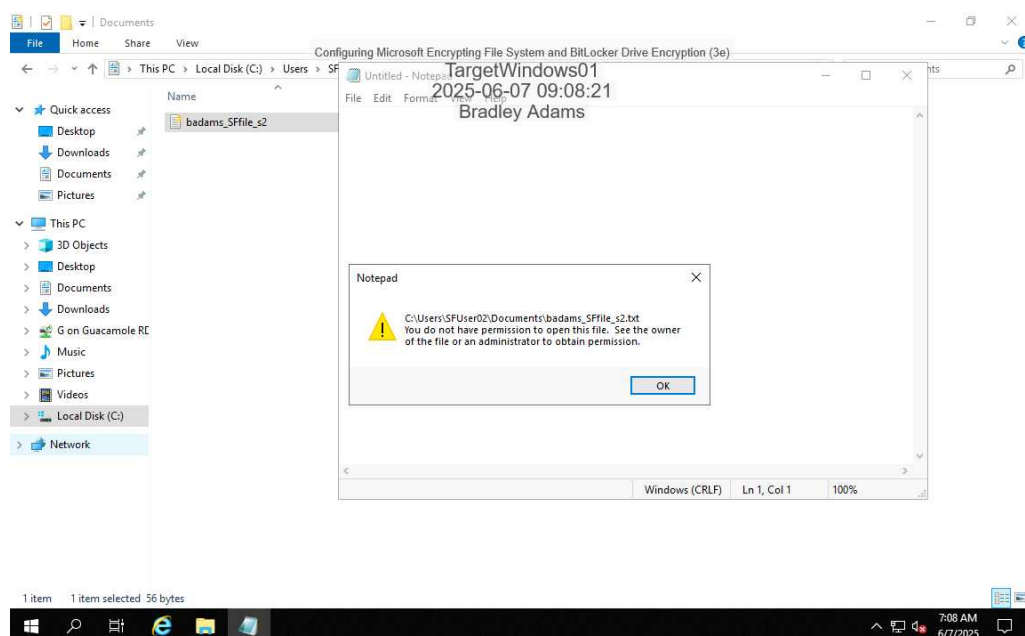## Section 2: Applied Learning

Part 1: Configure Microsoft Encrypted File System (EFS)

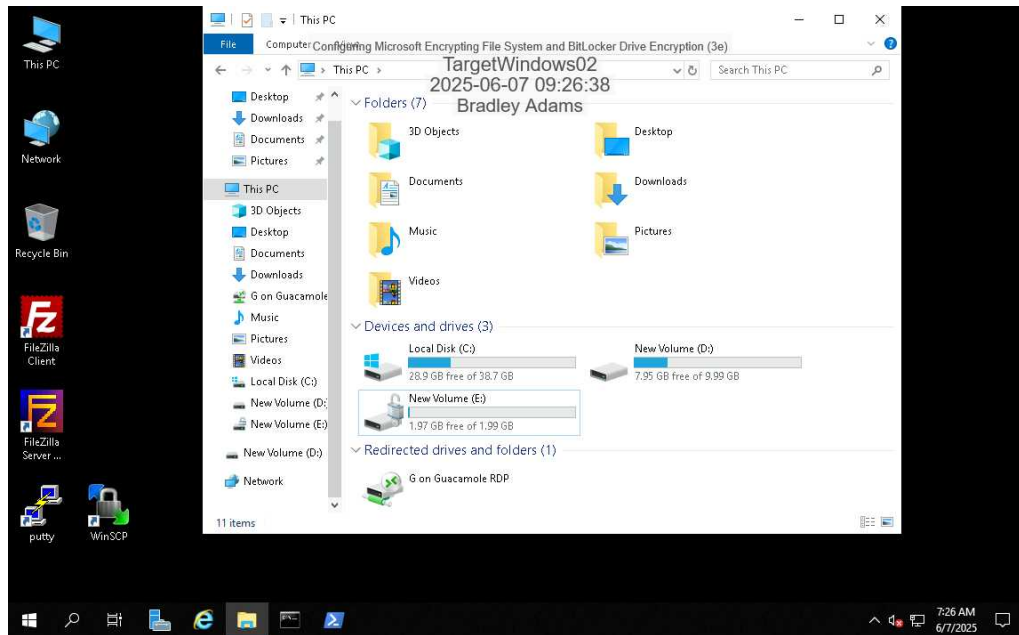6. **Make a screen capture** showing the **encrypted SFUser02 Documents folder**.

Part 2: Test the EFS Security

4. **Make a screen capture** showing **Notepad and the error message**.
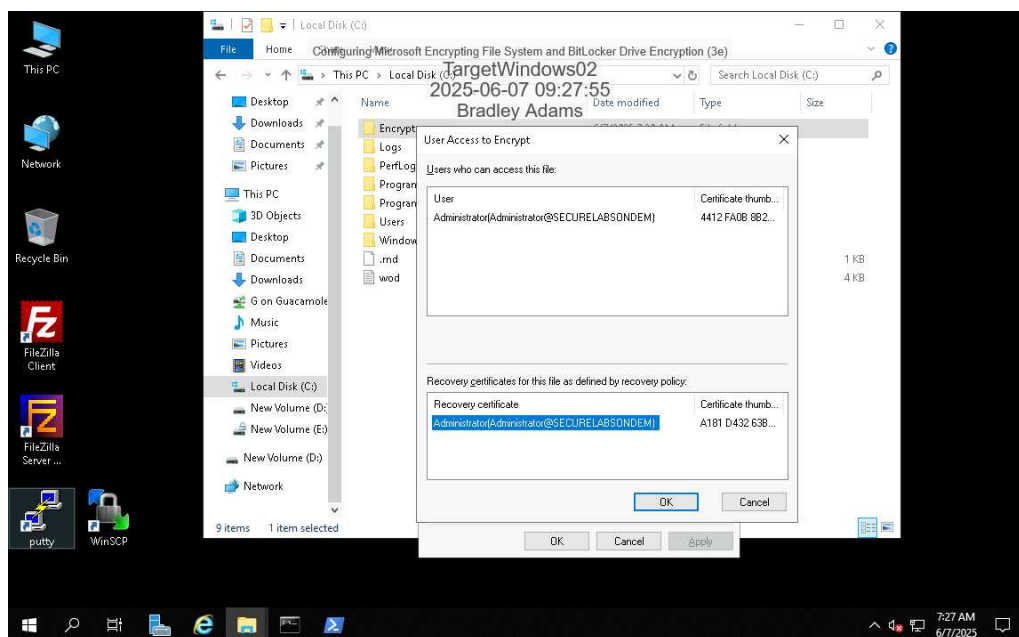
Part 3: Configure BitLocker

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?

As a veteran law enforcement officer having used forensic tools for discovering, processing, and presenting evidence for criminal prosecution, my opinion is admittedly biased as these tools help protect children from such criminals as those involved in child sex trafficking, abuse, and exploitation. These tools help protect all citizens from various crimes, as most crimes can have some digital evidence associated with them. I understand but disagree with the perspective from privacy advocates that these tools can be misused and that Microsoft should not have created them. Misuse of these tools should not be tolerated and usually presents criminal and /or civil liability for anyone who misuses the tools. I agree with the statement, "Security is an Illusion." A defense-in-depth approach is best, but a search warrant signed by a judge is powerful.

Part 2: Tools and Commands

Make a screen capture showing the **PowerShell command(s) used to unmount the E: drive**.
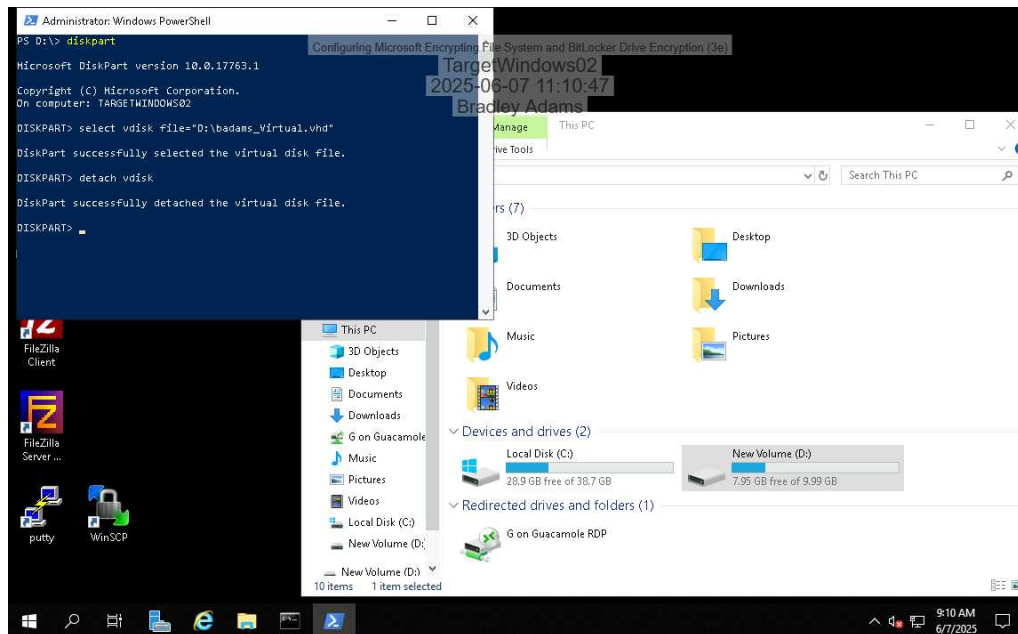
Part 3: Challenge Exercise

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