File Recovery

Objective: In this lab simulation, I demonstrate the process of recovering deleted files in an Active Directory environment using Windows shadow copies and previous versions. This lab focuses on restoring accidentally deleted user data and ensuring business continuity through built-in file recovery tools.

Equipment: Ticketing System, Windows Server 2022, and (2) Windows 10 PC

Ticket: Please look at page 2

Steps: Please look at page 3

Real World Tickets

Incident Details:
Incident #. 32849
Category: File Recovery
Department: Sales
Priority: Critical
Assignee: Helpdesk Team
Date/Time Opened: 8/22/2025 3:05 PM

Description:

User reports accidentally deleting important files from a shared network folder and requests assistance in recovering them. The user needs the files restored as soon as possible to continue working on an ongoing project.

Solution:
Incident #. 32849
Steps Taken:

1. I remotely accessed the user “Daniel’s” PC to see if the file deleted was in the recycle bin
2. Upon checking his recycle bin, it was not there
3. I went to the shared mapped network drive and clicked “restore previous version”
4. The latest previous version that was available for the folder was on “8/22/2025 2:58 PM”
5. Upon restring the folder to the most up-to date version, Daniel was able to recover that file that was deleted

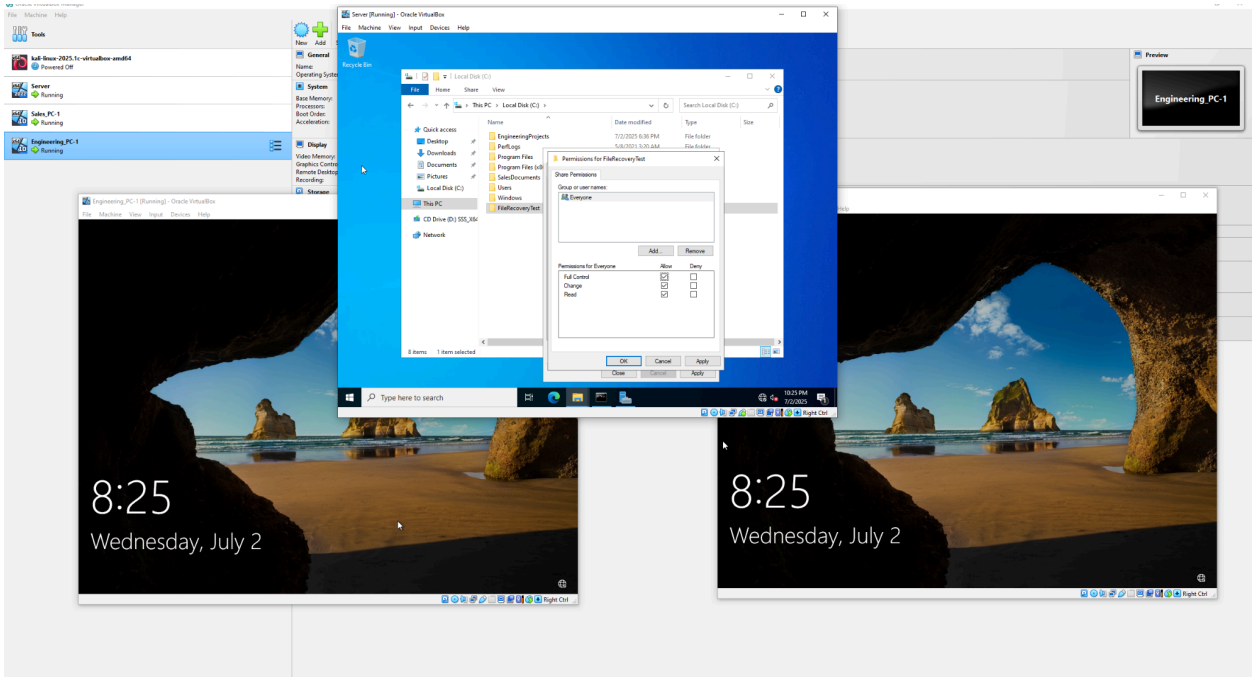
Notes:

- File was not in the recycle bin
- I restored the folder that contained the file to a version that was last snapshotted at “8/22/25 2:58 PM”
- Daniel was able to access the file

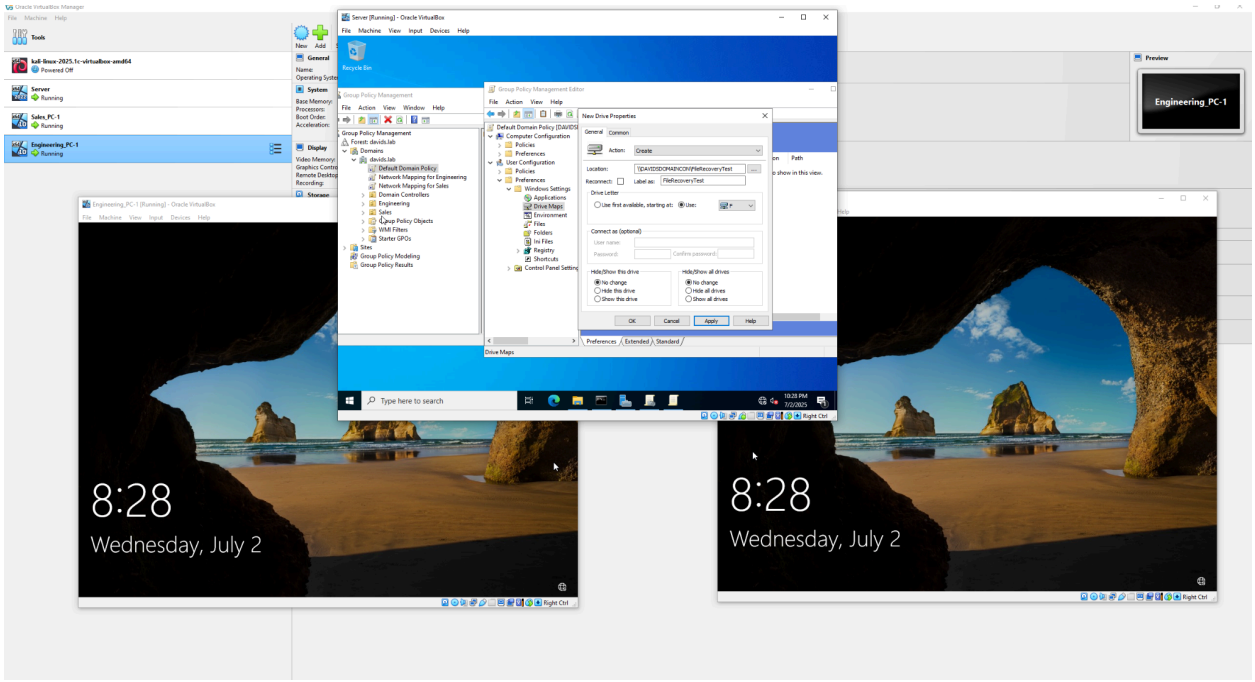
Time Logged: 7 minutes (3:05 PM - 3:12 PM)
Status: Resolved and Closed

Steps

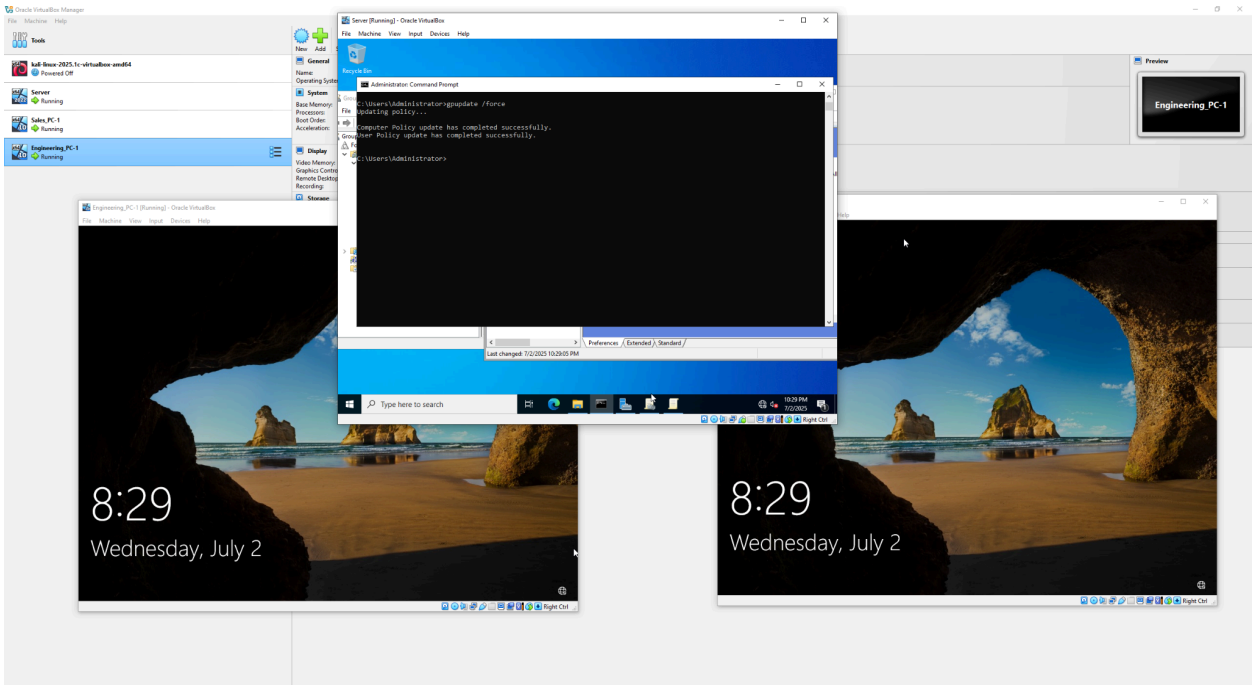
1. Make a file on the C: drive on the windows server and let everybody access the folder in the domain



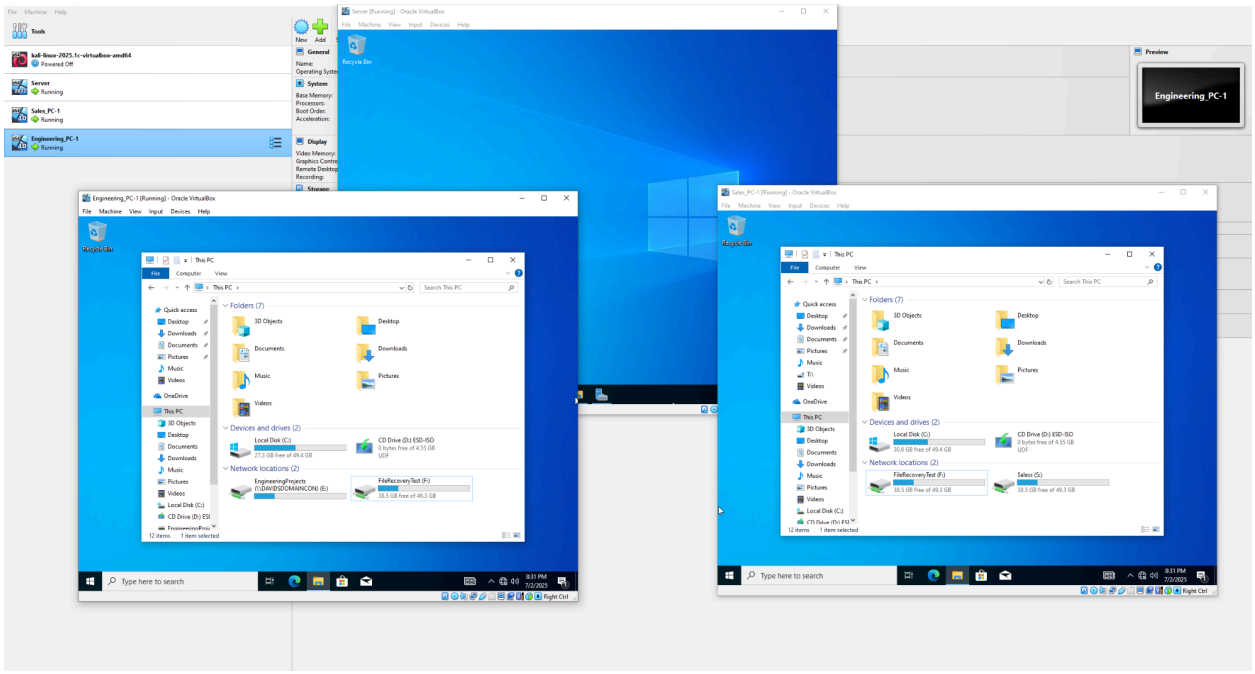
2. Create a default policy GPO mapped drive so everybody in the domain has easy access to it



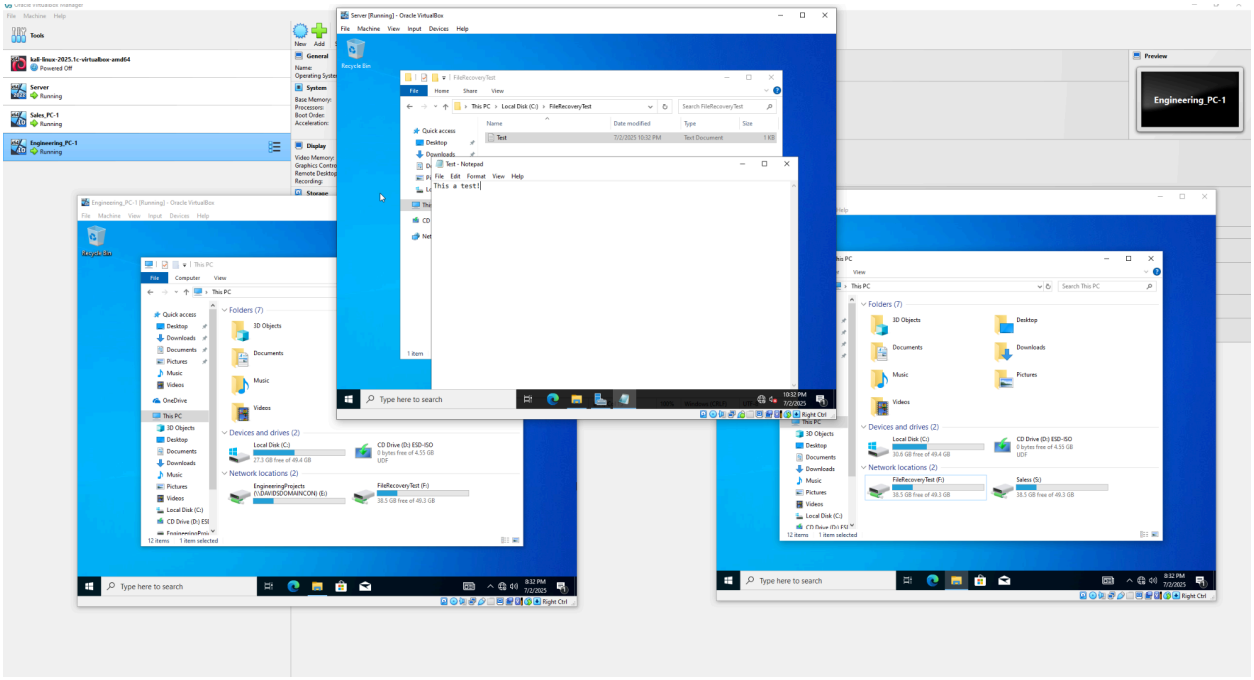
3. Force update the GPO



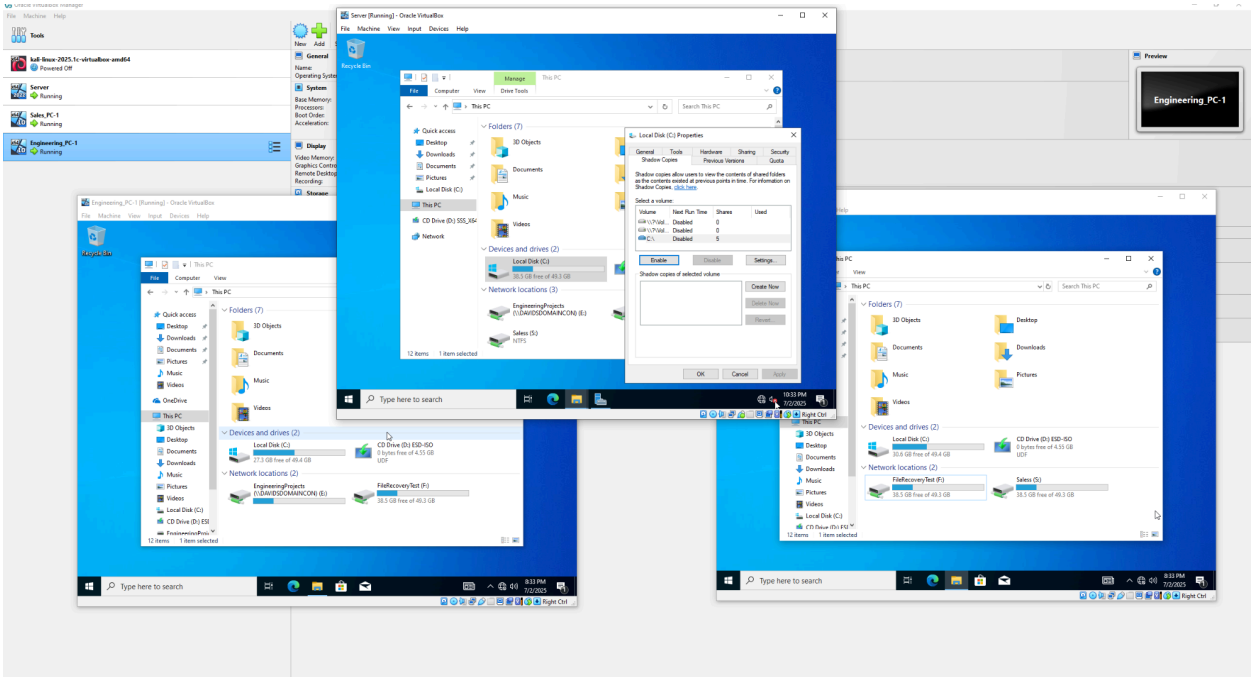
4. Ensure everybody has access to it



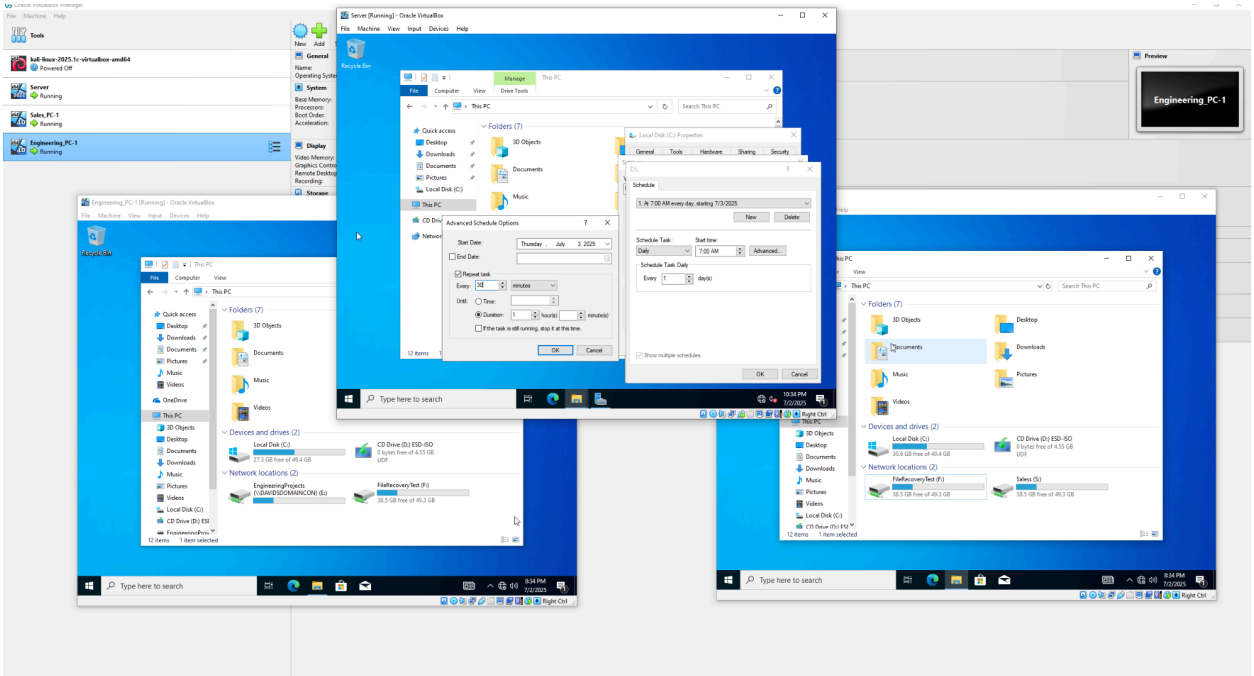
5. I created a simple TXT file to simulate an important file about get deleted



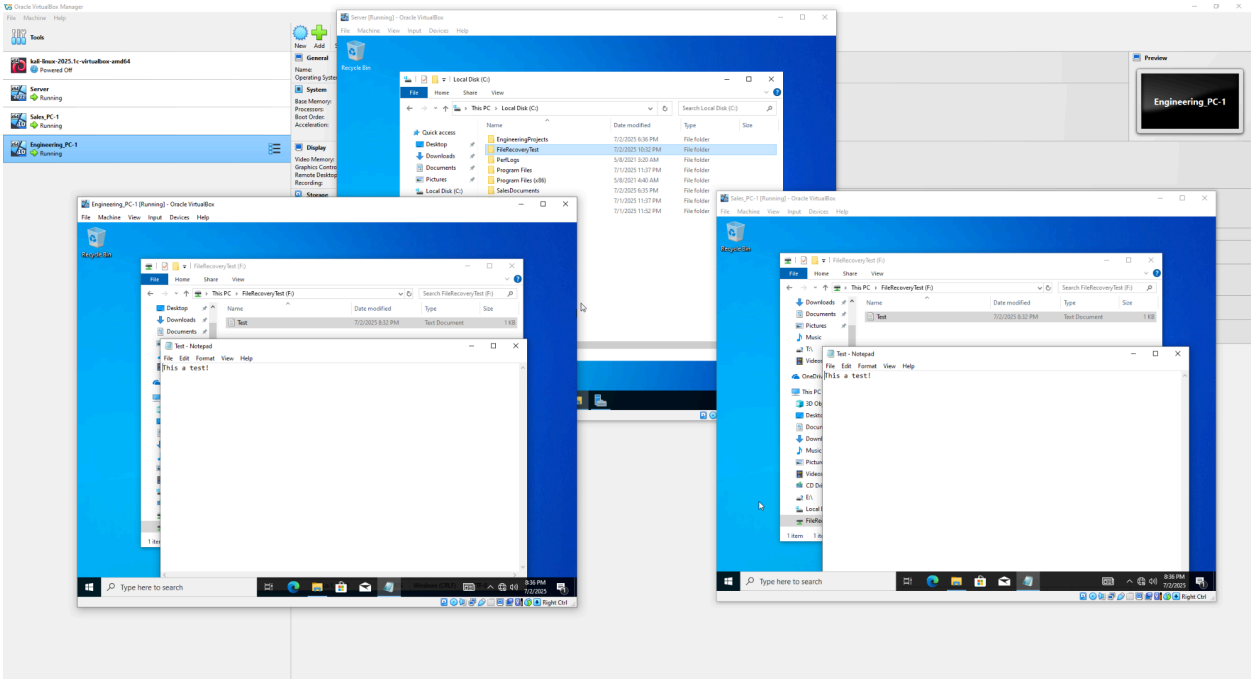
6. I enable shadow copies on the C: drive to backup folders/files



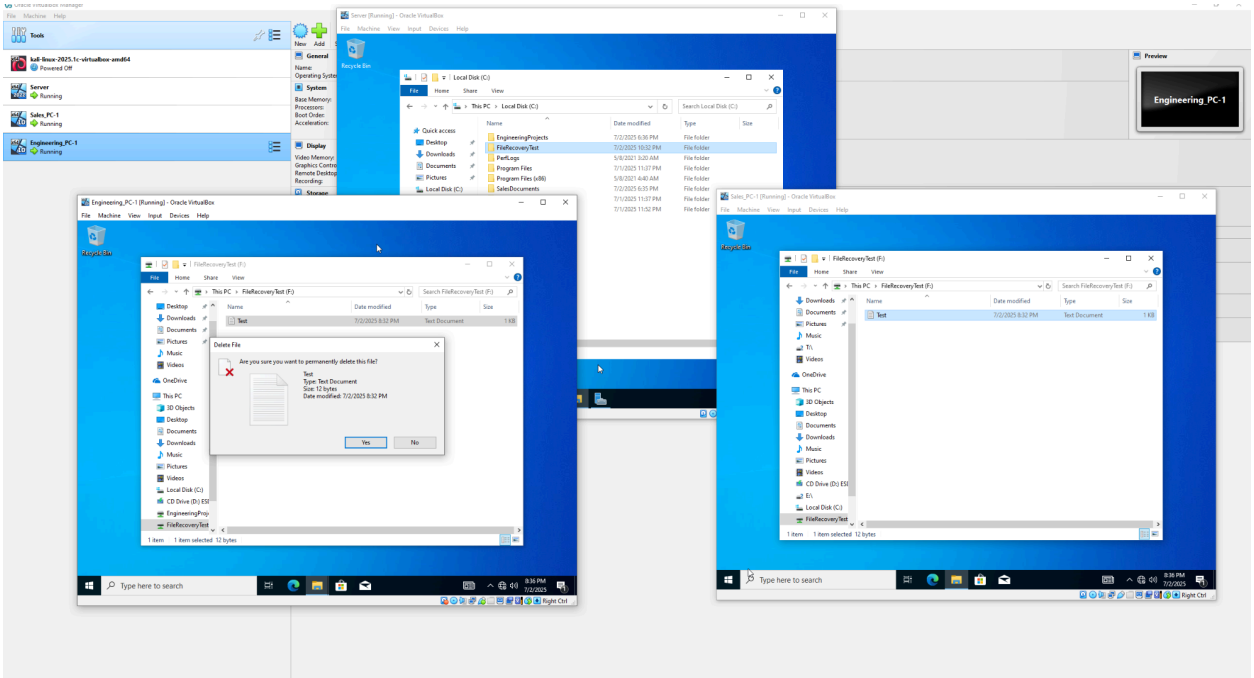
7. I set a schedule to take a snapshot every 30 minutes



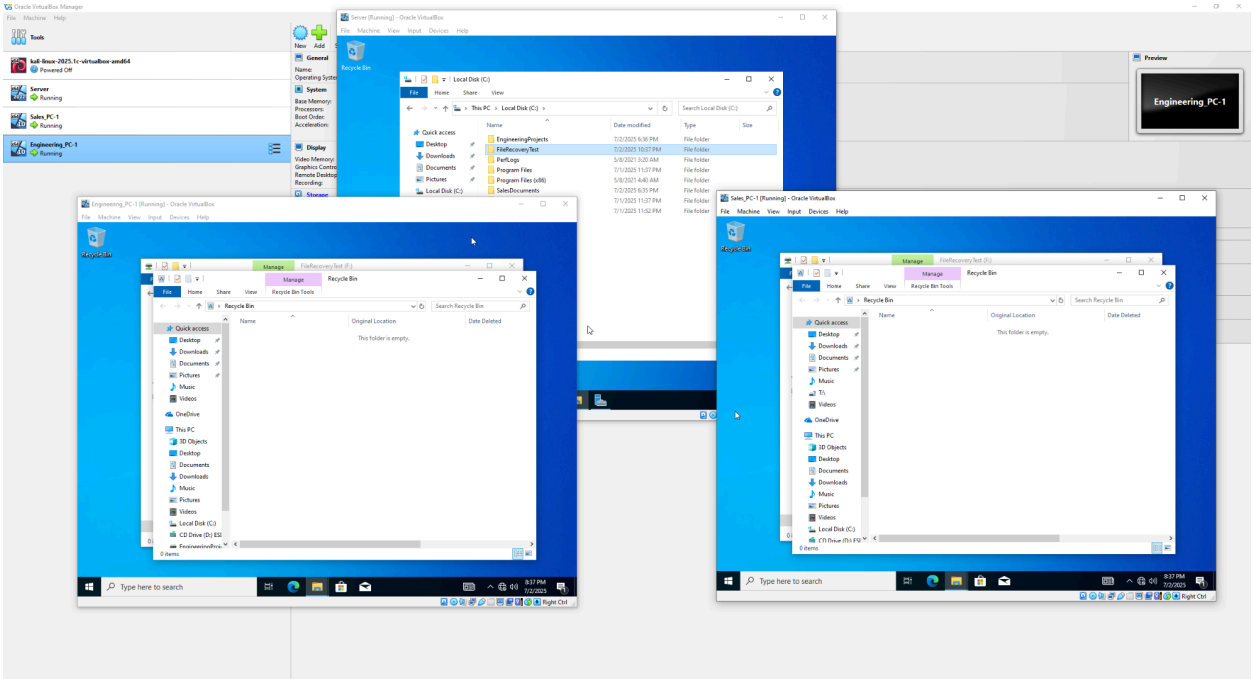
8. I ensure that the file exist for both parties



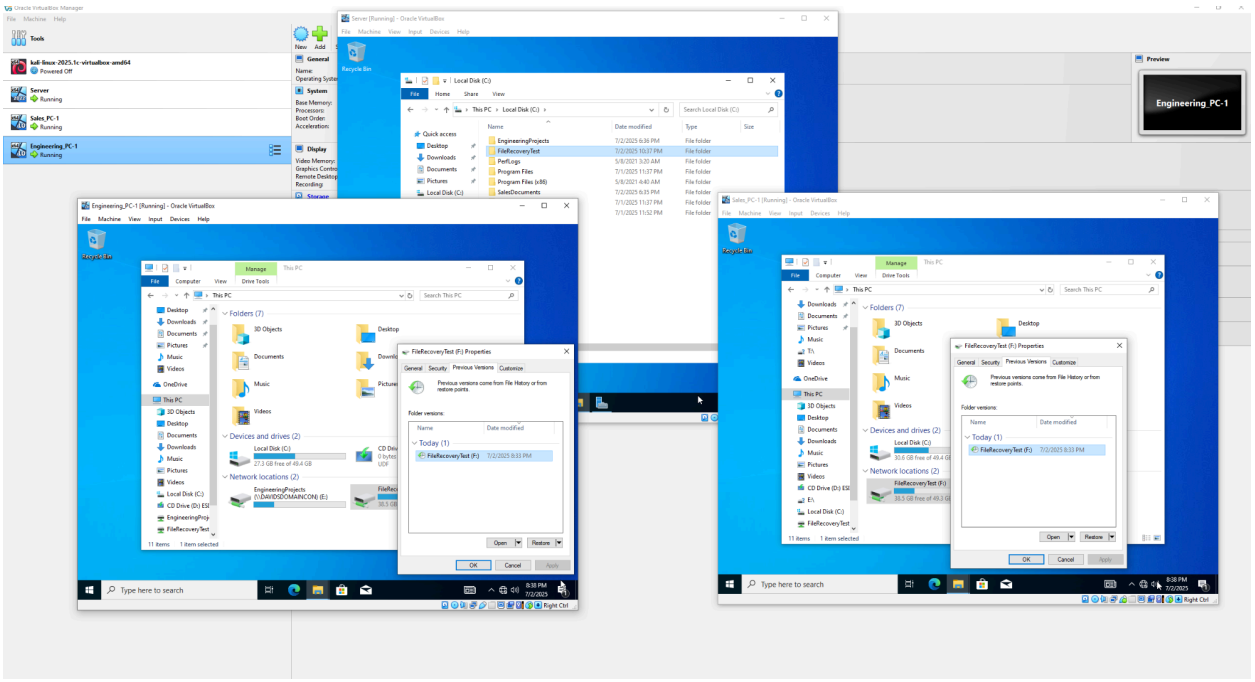
9. I deleted the file from one of the users



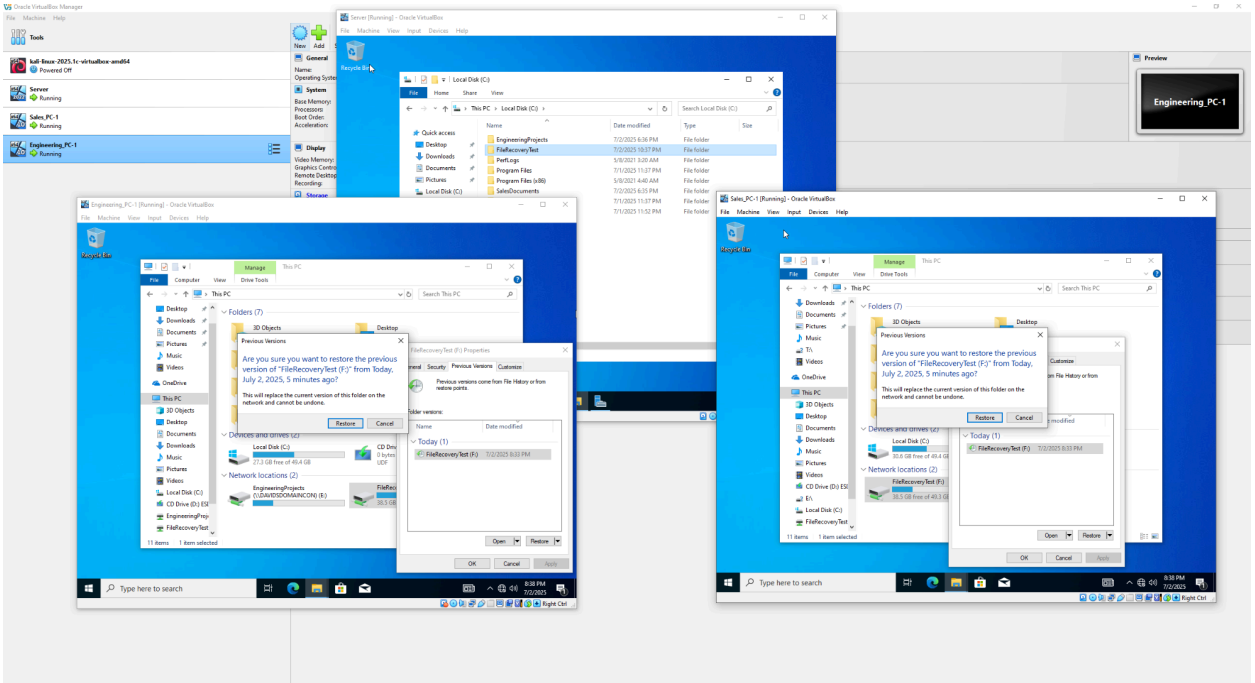
10. File is deleted for both users



11. I use the previous version to see if the snapshot worked, which it did



12. I restored the folder to a the latest previous version



13. File was recovered successfully