How to Restore Individual Organizational Units and User Accounts AFTER They've Been Deleted

- The Two Types of Restorations
  - Use Windows Server Backup to do a Non-Authoritative Restoration
  - Use NTDSUTIL and WBADMIN to do an Authoritative Restoration

Things are going well, until on a Tuesday morning the entire New York Ops department can no longer log in. When you go to see what's happening, you notice that the New York Ops OU is...gone. Aced, no trace, nada, not there, here or anywhere.

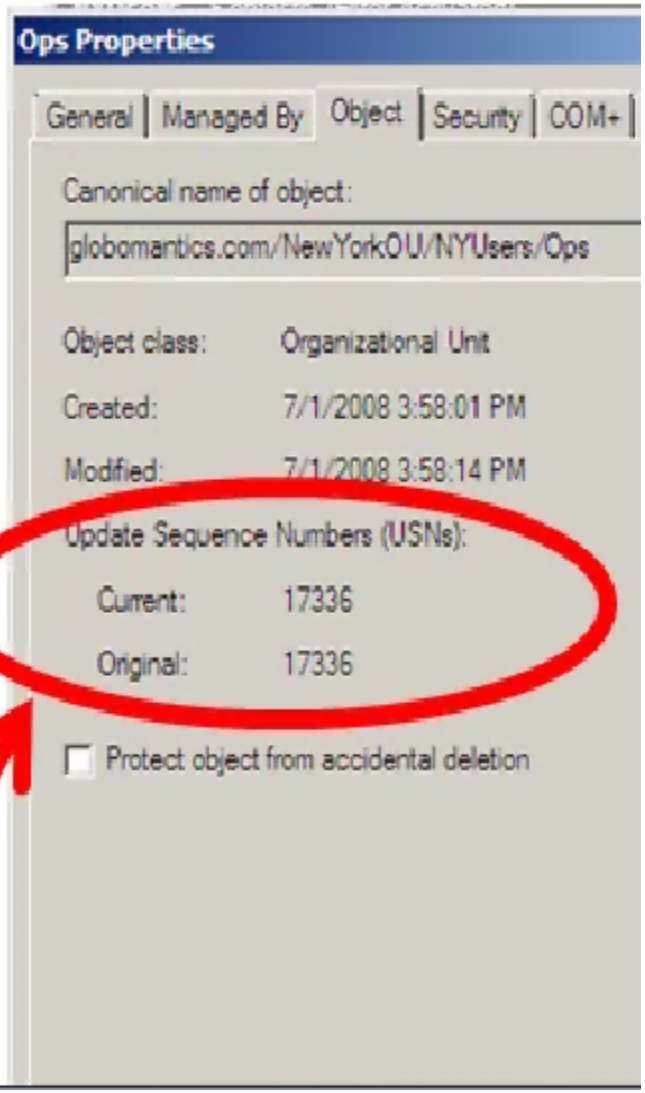
When you check your Security log, you see that the account B5amson, an account belonging to one of your new IT staff who had been given Account Operator permissions, successfully deleted the entire OU last night at 1AM. Brock did not report in this morning due to the fact that he's in police custody for *ahem* other chemically-related issues.

There are two options for doing restoration of an OU:

- Non-Authoritative Restore: Most often done using Windows Server Backup, you can restore the entire Domain Controller.
- Authoritative Restore: Using WBADMIN and NTDSUTIL, you can restore an OU, an individual User Account, or any other AD Object after doing a System State Restore and mark it as Authoritative.

What makes a Restore "Authoritative?"

- The Update Sequence Number in the AD Database is increased by 10,000 so other Domain Controllers know that the restored object is the most recent



- To run a non-authoritative restore, just go to Windows Server Backup and click Recover. Use the most recent backup file set that was created before the deletion. You're done (sort of-you may have problems with this type of restore).
- To run an authoritative restore:
  1. Restart the DC into Domain Recovery Mode (hit F8 on the keyboard during reboot to get this option)
  2. Login with ./Administrator and the Domain Recovery Mode password you set up when you ran DCPromo
  3. Type wbadmin get versions –backuptarget *backuplocation*, where backuplocation is the location where your back up files live
  4. Figure out which version you want to restore.
  5. Type wbadmin start systemstaterecovery –version:ID –backuptarget: *backuplocation*
  6. After the restore, type ntdsutil activate instance NTDS
  7. Type authoritative restore to get into the right NTDSUTIL Context
  8. Type restore object "*distinguishedName*" for a single account or restore subtree "*distinguishedName*" if you're restoring an entire OU.
  9. Reboot normally.