COPS Guide - Data Transfer (Windows)

contributors: shaun@	*updated: 04-JUL-2024*

Backup

- Restart Windows
  > *Force Restart Windows (`shutdown -r -f -t 00`) now to provide a clean slate for proceeding*
- Disable Antivirus
  > *Some of our extraction tools prompt false positives in most security packages*
- Create a Job# number folder on a Transfer Drive
  > *Create a new folder with the current job number (ie. 'Job#5000') to save User Data to*
- User Profile
  > *use Forensit Transwiz, Fast Pack (no compression), use default filename*
- Web Browsers
  > *For each web browser installed export the following:*
  - Export Bookmarks *(ie. 'Web Browser - Google Chrome - Bookmarks - 2024-07-15.html')*
    > *Google Chrome URL:* `chrome://password-manager/passwords` *or* `chrome://settings/passwords` *(older versions)*
    > *Microsoft Edge URL:* `edge://favorites`
    > *Mozilla Firefox Hotkey:* `Ctrl+Shift+O`
  - Export Passwords *(ie. 'Web Browser - Google Chrome - Passwords - 2024-07-15.csv')*
    > *Google Chrome URL:* `chrome://password-manager/passwords` *or* `chrome://settings/passwords` *(older versions)*
    > *Microsoft Edge URL:* `edge://wallet/passwords` *or* `edge://settings/password s` *(older versions)*
    > *Mozilla Firefox URL:* `about:logins`
- Installed Programs *(ie. 'Installed Programs - 2024-07-15.html')*
  > *use Nirsoft UninstallView, save all as Horizontal HTML*
- License Keys *(ie. 'License Keys - 2024-07-15.htmal')*
  > *use Nirsoft ProduKey and Nirsoft Product Key Scanner*
- Check C: Drive for unusual files/folders
  > *copy to Job folder copying the C: Drive file structure (TransferDrive:\Job#5000\C\FolderToSave)*
- [OPTIONAL] Create Winget Install Script
  > *https://winstall.app/ - Select Desired Programs - Generate Script - Download both Batch (.bat) and PowerShell (.ps1) scripts*
- Drivers *('TransferDrive:\Job#5000\Drivers - 2024-07-24')*
  > *Open PowerShell as Administrator and run (update with your export folder location):*
  > ```
  > Export-WindowsDriver -Online -Destination REPLACE-WITH-EXPORT-FOLDER
  > ```
- Enable Antivirus
- Create a System Restore point

Restore