mft2csv

ntfs log tracker - blue angel forensic

md5 calculator - bullzip

total recall data recovery software

md5sum

hashmyfiles calculate md5 sha - https://www.nirsoft.net/utils/hash\_my\_files.html

exiftool phil harvey

exiftool.exe -csv photos > exif.csv

exif data viewer  -  <http://www.softsea.com/download/Exif-Data-Viewer.html>

PC Inspector File Recovery

**Wild Card Syntax:**

? = Replaces any single character in the file name and extension

\* = Replaces any series of characters in a file name and extension

| = Separates directories and files

**Wild Card Filters:**

Users|\*|NTUSER.dat

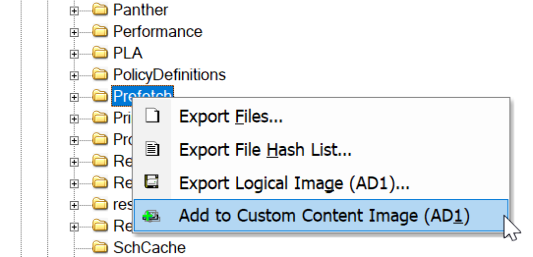
Users|\*|Documents|\*.doc

Users|\*|Downloads|Evidence ?.pdf

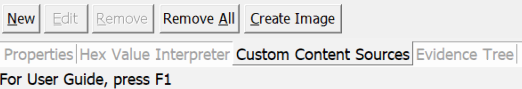
Windows|Prefetch|\*

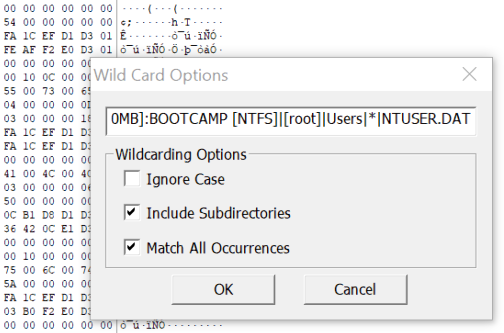
**1:** Start by browsing to your custom content item.

**2:** Then right-click and select add to “Custom Content Image”.



**3:** You can manually add custom content by selecting “New” using the wildcard option or “Edit” existing custom content.





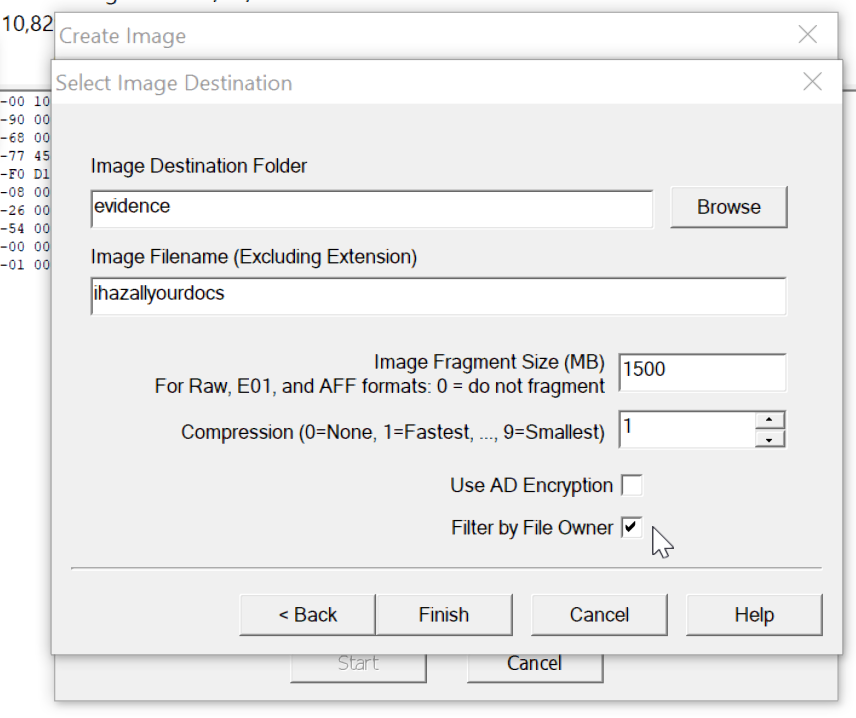
\*As far as I’m aware, there is not an option to save your custom content as a template.

(Please let me know if you do, as I currently just use a text file as a template for files of interest for varying investigation types)

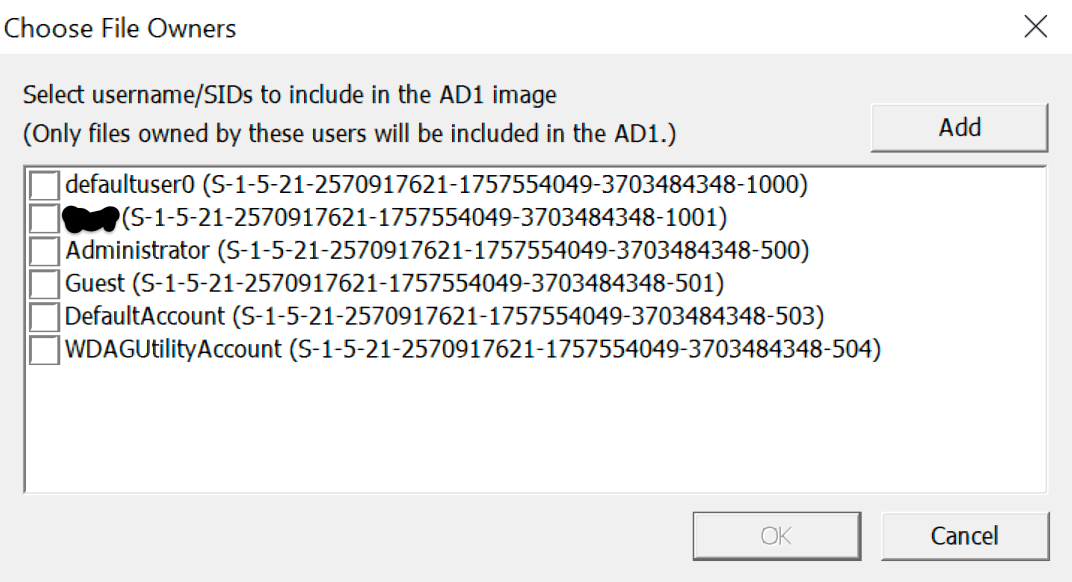
## Creating Content Image by User SID

As previously mentioned, your scope may be limited due to shared computer use and while this may not be of too much importance for law enforcement, files belonging to a user may be marked as privileged by civil court orders.

We can use FTK Imager to create an image of only files owned by a specific users SID, the process is just as we defined previously but upon creating the custom content image you need to select the tick box to “Filter by File Owner”.



Once you have selected this, you will be presented with the respective file owners and their SID’s on the system.



## Collection for Incident Response

The last instance where these methods may be useful is if you have a handful of workstations where you need to collect some very specific files or artefacts from. I tend to use a text file as a template. Although this works, it is a bit clunky and slow.

There are a great many other commercial and open source tools which can already perform these tasks extremely well, such as f-response, X-Ways Forensic, GRR and so on. This option also doesn’t really work for incident response at scale but if you’re stuck without your commercial tools or have a very targeted approach for collections from a few computers, then this could work for you.

FTK Imager also comes in a lite flavour which doesn’t require any installation.

Reference:

<https://support.microsoft.com/en-au/help/243330/well-known-security-identifiers-in-windows-operating-systems>

<https://accessdata.com/product-download>

<https://www.f-response.com/>

<https://github.com/google/grr>

