Obtaining & Accessing Protected Registry Files

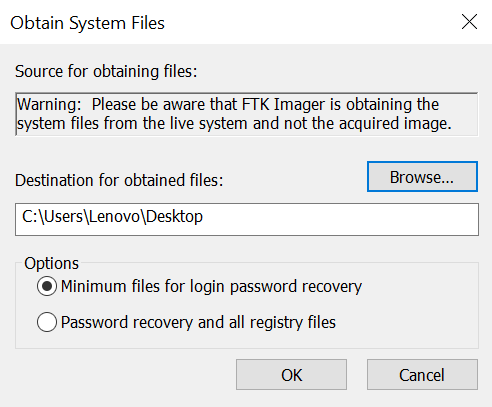
The Windows operating system does not allow us to copy or save live Registry files. Without FTK Imager, users have had to image their hard drive and then extract the Registry files, or boot their computer from a boot disk and copy the Registry files from the inactive operating system on the drive. FTK Imager provides a much easier solution. It circumvents the Windows operating system and its file locks, thus allowing us to copy the live Registry files.

### Acquiring Protected Registry Files on a Local Machine

### We can acquire the Protected Registry Files using FTK Imager running on the machine whose Registry files we need.

To acquire Protected Registry Files on a local machine

1. Launch FTK Imager.
2. Do one of the following:
   * Click File > Obtain Protected Files.
   * Click the **Obtain Protected Files ** button on the *Toolbar*.
3. Specify a destination directory.
4. Select the option that suits our needs:
   * *Minimum files for login recovery*: Retrieve Users, System, and SAM files from which you can recover a user’s account information.
   * *Password recovery and all Registry files*: Retrieves Users, System, SAM, NTUSER.DAT, Default, Security, Software, and Userdiff files from which you can recover account information and possible passwords to other files. This list can also be imported to the AccessData password recovery tools, such as PRTK, and DNA.
5. Click **OK**



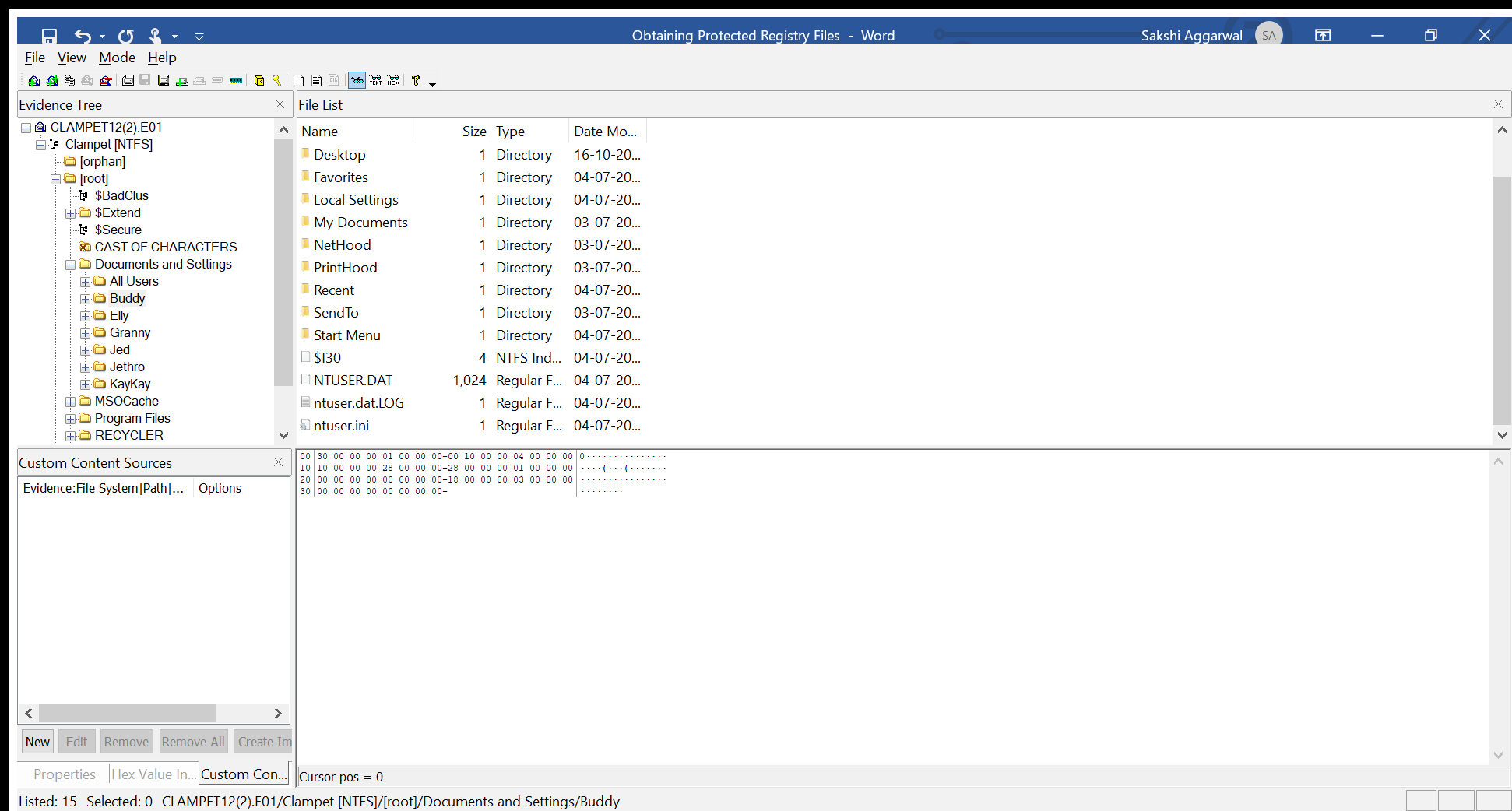
1. FTK Imager exports the selected files to the designated location.

### Accessing Registry files from a Drive Image

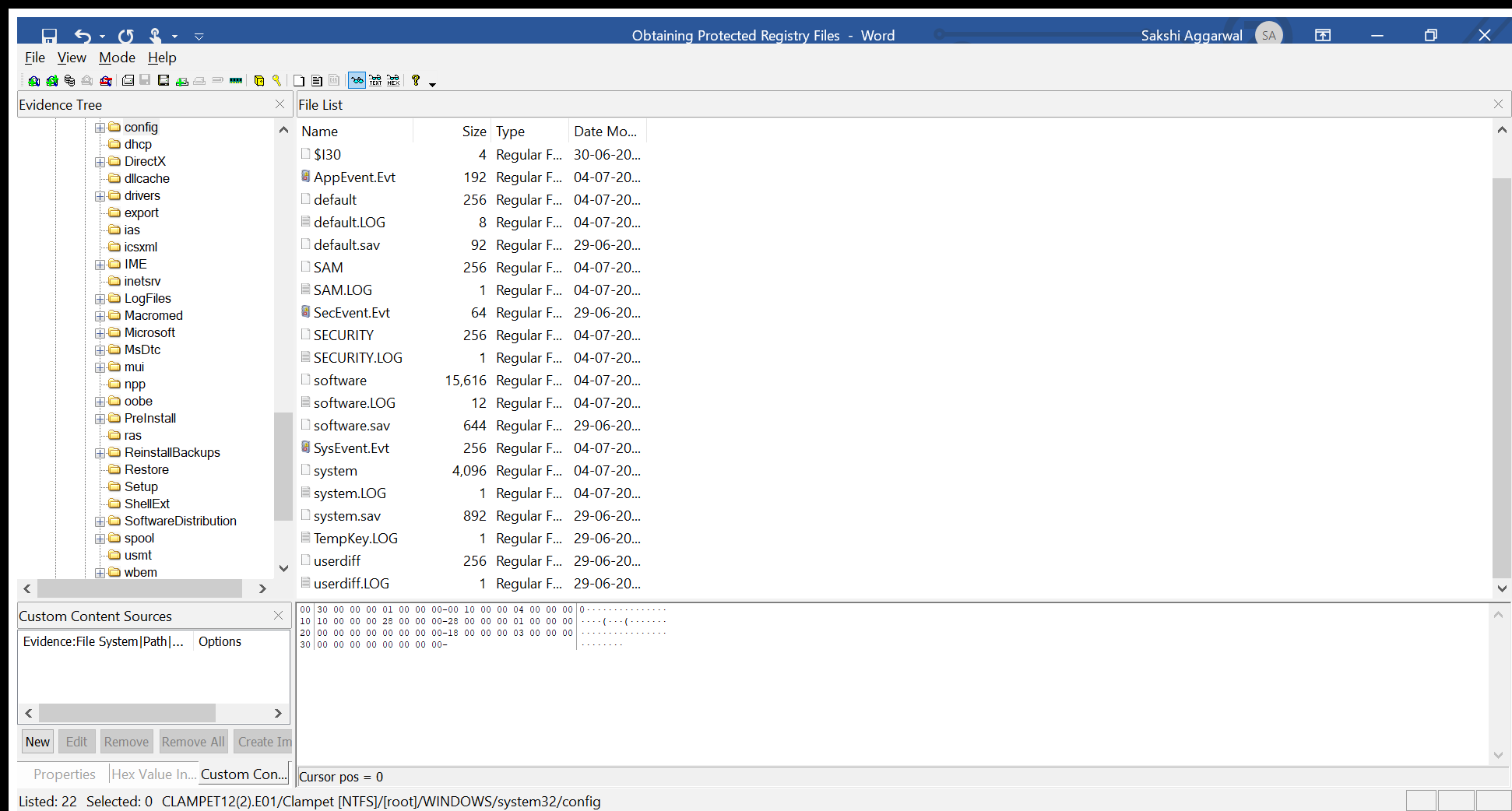
### Registry files can be accessed from the Registry viewer (another tool). Registry files can be exported from the image file in FTK Imager.

In XP

1. Navigate to [Image]:\Documents and Settings\[username]\.
2. Export
   * ntuser.dat



1. Navigate to [*Drive*]:\Windows\System32\Config\.
2. Export the following files:
   1. SAM
   2. System
   3. Software
   4. Security



Regardless of the operating system, export the files to an accessible location, then add/open them one at a time in Registry Viewer to view the content of the file.