Lab 1 – Securely wiping a USB Drive

Deleting a file only deletes the pointer to the file. The MFT table (Master File Table), which stores the physical location of files in file systems is updated to reflect the free space. Therefore deleted data may still reside on a computer.

Forensics software can recover file remnants and reconstruct an original file by a process called 'Data Carving'. Secure destruction of digital data often requires writing a series of 1's or 0's to the store device to overwrite any file remnants. NIST requires seven wiping passes

Activity

1. Log into your VM, and insert a USB drive containing files you don't need.
2. Right click on ProDiscover icon and click Run as Administrator. Click Yes on the User Account Control (UAC) message box.
3. Click the "Don't show this dialogue in the future" box and then click Cancel to close.
4. Click Tools, Secure Wipe from Menu
5. Click the Disk to Wipe list arrow and click the drive letter corresponding to the USB drive. **Double check before you proceed that you have the correct drive selected to prevent accidental erasure.**
6. In the number of passes box, type 7 and then click Start to begin
7. Click OK on the warning box. The Securely Deleting file message is displayed in the lower left corner to indicate process has begun.
8. This will take at least 60mins or more.
9. A message will be displayed when the process is complete. Click OK to exit ProDiscover.
10. Click NTFS in the file system list box and type EVIDENCE in the volume label text box. Click Start to format the USB drive. Click OK in the Format Removable Disk message box.
11. When the format is finished, click OK and close the dialogue box. Copy the 11 files from the C2Proj1 folder onto the USB stick. Label the device and don't write anymore files to it.
12. Close all windows.

Lab 2 – Using ProDiscover to Image a USB Drive

Disk imaging builds forensically sound bit-for-bit copies of the evidence data, including tye MFT and all physical file locations containing data or remnants and unallocated free space.

This allows the original device and evidence to be protected. In this lab, an image file (.eve) will be built. This process mirrors what would happen in a real investigation except in a real investigation a write blocker would be used. A Write Blocker is a piece of hardware or software inserted between the original device and the machine creating the image to prevent the original being overwritten, which violates chain of custody.

Activity

1. Insert the USB drive containing the Evidence (prepared in Lab 1).
2. Create a folder called Work and then create a subfolder called Labs. The Work\Labs folder will be used throughout the course. Create subfolders Cases, Data and Evidence.
3. Open ProDiscover. Click Action, Capture Image from the Menu.
4. In the Capture Dialogue box click the Source Drive list arrow and then click drive letter of USB.
5. Click the double arrow button next to Destination test box, click Choose Local Path and navigate to the **Work\Labs\Evidence folder**. In the Save as box type C2Proj2 in the filename text box and click Save.
6. In the Capture Image Dialogue box, type your full name in the Technician Name text box and type C2Proj2 in the Image Number text box. Click OK to continue.
7. When imaging finished, click OK. Go to the **Work\Labs\Evidence folder** and confirm the image file (C2Proj2.eve) has been created.
8. Close File Explorer and exit ProDiscover.

Lab 3 – Converting a ProDiscover Image to a .dd Image

Forensics Investigators will often use many different tools to search for evidence but also they may use different Image tools depending on their needs and how fast they want the data as some tools work faster than others, depending on file formats (NTFS/HFS).

Most tools only produce Image files that they can read (they are not compatible). ProDiscover produces images in .eve but ProDiscover can convert to other formats such as .dd (and this format is supported by most tools). The .dd format produces a bit-by-bit copy of a storage device's content and can be ready by Windows, Linux, UNIX and Mac.

ProDiscover also allows for the conversion of .eve images to ISO, .dd to ISO and .dd to VMware. ISO images are files stored in uncompressed format.

We will now convert a ProDiscover image to .dd format so we can use it with FTK in the next Lab.

Activity

1. Open ProDiscover. Click Tools on the menu, point to Image Conversion Tools and click Convert ProDiscover Image to DD.
2. In the dialogue box, click the browse button and navigate and click on the Work\Labs\Evidence folder and click on C2Proj2.eve file.
3. Click OK. The blue indicates progress of conversion.
4. When finished navigate to Work\Labs\Evidence folder and that the C2Proj2.dd image has been created. The image file size should be approximately the size of the storage device not the data.
5. Close all windows and exit ProDiscover.