F20FO/F21FO - Digital Forensics

Lab 02: Digital Forensic Foundations

Lab 2: Objectives

1. Install Windows VM
2. File & folder properties
3. Software write blocker
4. FTK Imager

Notes

There is nothing to submit at the end of this lab, however students are encouraged to log and record their certificate and results in a document. There are some questions coloured in blue that you can use as indication to record in your logbook (e.g. lab02_logbook). Often the lab instructions are intentionally open ended, and you will have to figure some things out for yourselves.

There are some new topics in this lab, these are covered in the lecture, and in more depth in future lectures. The lab will require you to install software and download some forensic evidence. The lab is based on Windows. Changes to your machine should not impact on its functionality - however you are recommended to use a VM.

Lab 2.1: Install Windows VM

You will need to add an instance of a Windows 10 Virtual machine to your VirtualBox from Lab01. You can download a VirtualBox Windows 10 VM from this link:

MSEdge.Win10.VirtualBox.zip

Note: The Windows VM is valid for 90 days. If you plan to re-use the Windows 10 VM again, it is recommended to take a snapshot of the VM when first added to VirtualBox.

The username and password for the Windows 10 VM is:

User: IEUser

Password: Passw0rd!

Alternatively, you can download the Windows 11 iso from this link

Win11_25H2_EnglishInternational_x64.iso

and install in your VM software. It is recommended to use 4GB RAM and at least 60GB disk space. Selecting "Custom Install" and skip entering a product key to use it inactivated initially. Take a snapshot of the Windows VM after successful installation. You might need to install guest additions (e.g. VMware Tools or VirtualBox Guest Additions) for better integration of the VM. For optimum

performance, you need to ensure UEFI firmware settings are selected, either search online “how to enable UEFI firmware” or start CMD or Windows PowerShell in administrator mode and type “`shutdown /r /fw /t 0`” and press enter, the Windows will restart with UEFI enabled.

Lab 2.2: File & folder properties

A file attribute is metadata that describes or is associated with a computer file. For example, an operating system often keeps track of the date that a file was created and last modified, as well as the file's size and extension (and what application to open it with). File permissions are also recorded.

To view more details about folders and file in Windows explorer a few settings have to be altered:

Open Windows explorer (Hold the Windows key and press E)

and Next click View > Options > Change folder and search options > View (as shown in Figure 1)

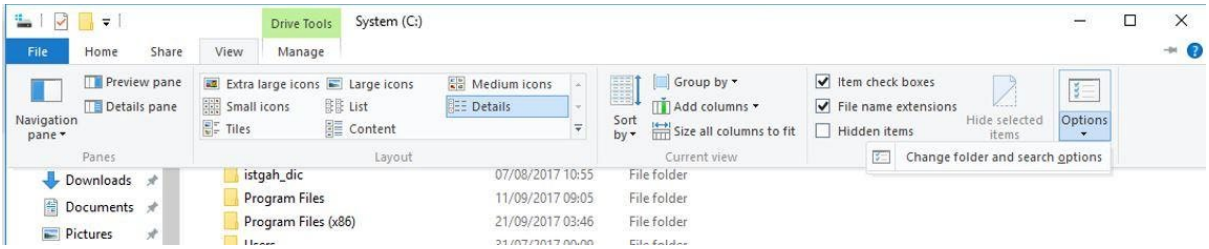


Figure 1: Windows Explorer Options

See Figure 2, Make sure you select Show hidden files, folders, and drives. Make sure you de-select Hide empty drives, Hide extensions for known file types and Hide protected operating system files. Click Apply to Folders > Yes > OK.

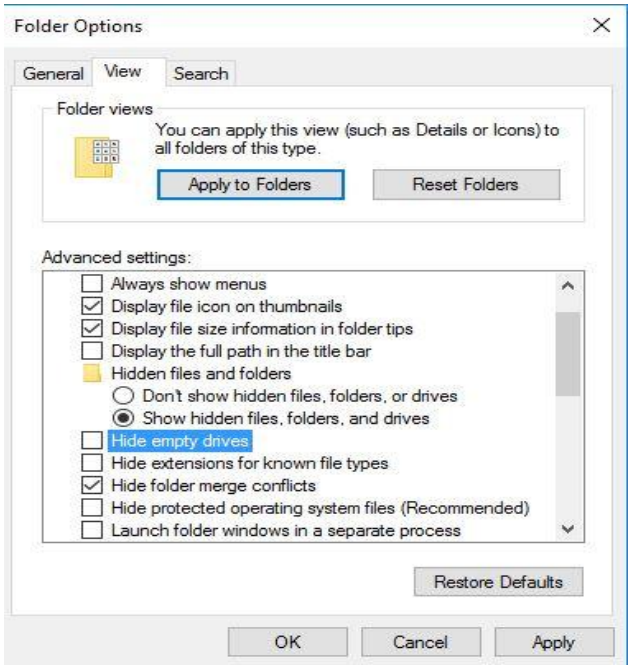


Figure 2: Folder Options

As an analyst, you need to display as much detail as possible including hidden files, system files and file extensions. Microsoft like to hide things from basic users.

For example, in your Local Disk (C:) you should now be able to see **hiberfil.sys, msdia80.dll, pagefile.sys** and **swapfile.sys**. Don't worry if you do not see all 4 files. hiberfil.sys, pagefile.sys and swapfile.sys are system files. As a basic user, you would not know these files were there. Knowing they are there, you can open them and may find some useful forensic information about the user.

Notice the information that you see in Windows Explorer. Above the main display window, you see 4 column headings – Name, Date modified, Type and Size (you may have to Minimise the Ribbon to see the column headings). Right click any column heading and select More. You can display many more columns than the four normally shown - some of these will be useful in some aspects of forensic analysis. You can see different sorts of dates, potentially useful if we want to build a chronology of events – and we know what those dates actually record, how they might get changed, and if they are in fact 'reliable'.

Lab 2.3: Software write blocker

In Windows XP Service Pack 2 (SP2) and onwards, a new feature was added by Microsoft to allow the write protection of USB block storage devices. This entails a simple Registry modification requires no hardware devices to write protect USB drives. This allows us to examine and duplicate USB devices with write protection.

To enable this feature, we will modify the Registry. As in all Registry operations, it is advisable to back-up your Registry files prior to modification. In Windows 10 or 11:

- Open the Start menu, do a search for Create a restore point, and press Enter.
- On System Protection, under Protections Settings, verify whether the setting is turned On or Off (see Figure 3). Local C: should be on (If System Protection is off, use system protection option to turn it on).
- Click on create and give a description to it, as shown in Figure 4.

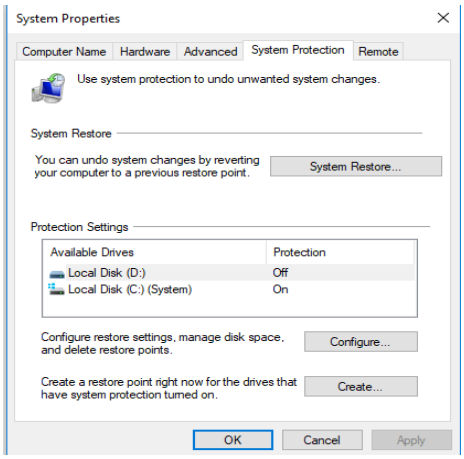


Figure 3: System Properties

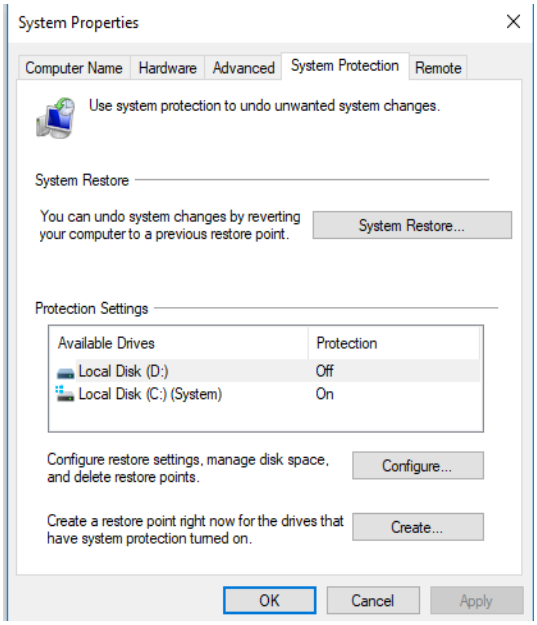


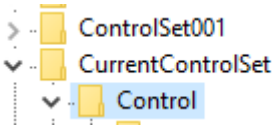
Figure 4: Create Restore Point

What does a system restore point do?

Write Blocker using registry key: To create the necessary Registry values to enable USB write protection, follow these steps:

Step 1 – Click on the 'search button' and look for 'regedit' and choose "regedit run command" and then choose "Yes".

Step 2 - Navigate to **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet** and highlight the Control key. The CurrentControlSet key has system information about the current configuration of the machine.

The system keeps a backup of this key. You will see the current and backup listed as **ControlSet001** in this example 

. The select key will show which is valid. The key **CurrentControlSet** is the one being used at this moment and is the one you want to modify.

Step 3 - Right click on Control and select **New** > **Key**. Name the key ***StorageDevicePolicies***. (if the Key is already there, delete it and try again).

Step 4 - Right click on **StorageDevicePolicies** and select **New > DWORD**. Name the value ***WriteProtect***.

Step 5 - Right click on **WriteProtect** and select **Modify**. To write protect USB devices select 1 as the value. To turn off write protection, change this value to 0.

We have created a new key and value in the Registry that will write protect USB devices. You may want to place this on your examination machine full time. However, if you need to be able to switch back and forth from a write protected state to a non-write protected state, it is cumbersome to have to go through this procedure each time. To automate this process, create a .REG file to enable you to select either on or off.

To create a write protect switch, Right-Click on **StorageDevicePolicies** and select Export. This creates a .reg file that will apply this key to the registry when double-clicked. Save this file on your Desktop as 'USB Write Protection On'. Again Right-Click on WriteProtect and select Modify; change the value to 0. Right-Click on **StorageDevicePolicies** and select Export again. Save this .reg file on your Desktop as 'USB Write Protection Off'. Now simply double-click on either .reg file on your desktop to enable or disable USB write protection.

You have now created a software write blocker, preventing the use of writable USB's on your computer. If you have a USB drive give it a try (it is optional).

Lab 2.4: FTK Imager

FTK imager is a data preview and imaging tool that allow quickly assess electronic evidence to determine if further analysis with a forensic tool such as Encase, FTK is warranted. FTK Imager can also create perfect copies (forensic images) of computer data without making changes to the original evidence.

FTK Imager supports:

- Create forensic images of local hard drives, floppy diskettes, Zip disks, CDs, and DVDs, entire folders, or individual files from various places within the media.
- Preview files and folders on local hard drives, network drives, floppy diskettes, Zip disks, CDs, and DVDs
- Preview the contents of forensic images stored on the local machine or on a network drive
- Mount an image for a read-only view that leverages Windows Explorer to see the content of the image exactly as the user saw it on the original drive.
- Export files and folders from forensic images.
- See and recover files that have been deleted from the Recycle Bin, but have not yet been overwritten on the drive.
- Create hashes of files using either of the two hash functions available in FTK Imager: Message Digest 5 (MD5) and Secure Hash Algorithm (SHA-1).
- Generate hash reports for regular files and disk images (including files inside disk images) that you can later use as a benchmark to prove the integrity of your case evidence. When a full drive is imaged, a hash generated by FTK Imager can be used to verify that the image hash and the drive hash match after the image is created, and that the image has remained unchanged since acquisition.

Important: In real scenarios, when FTK Imager is used to create a forensic image of a hard disk or other electronic device, a hardware-based write-blocker should be attached between the forensic base station (PC) and the electronic device (the device under investigation). This ensures that the operating system does not alter the original source drive when it is attached to the forensic base station. To prevent accidental or intentional manipulation of the original evidence, FTK Imager makes a bit-for-bit duplicate image of the media. The forensic image is identical in every way to the original, including file slack and unallocated space or drive free space. This allows the store of the original media away, safe from harm while the investigation proceeds using the image. After an image of the data is created, a forensic investigation toolkit such as Encase, FTK or Autopsy is used to perform a complete and thorough forensic examination and create a report of the findings.

You have the choice to download the latest version of FTK Imager (version 4.7) or use the one provided in Canvas (Resources module):

- Download and install FTK imager from: https://go.exterro.com/l/43312/2023-05-03/fc4b78

You need to submit your details and a valid email address where the FTK imager download link will be sent to. Follow the link and install FTK imager, agree to the required fields.

Note that you can use the FTK installer that is provided in **Canvas (Resources module)** for this lab or from within your VM, you can download the FTK installer from:

http://tinyurl.com/FTK-imager

Familiarise yourself with the FTK Imager interface (see Figure 5).

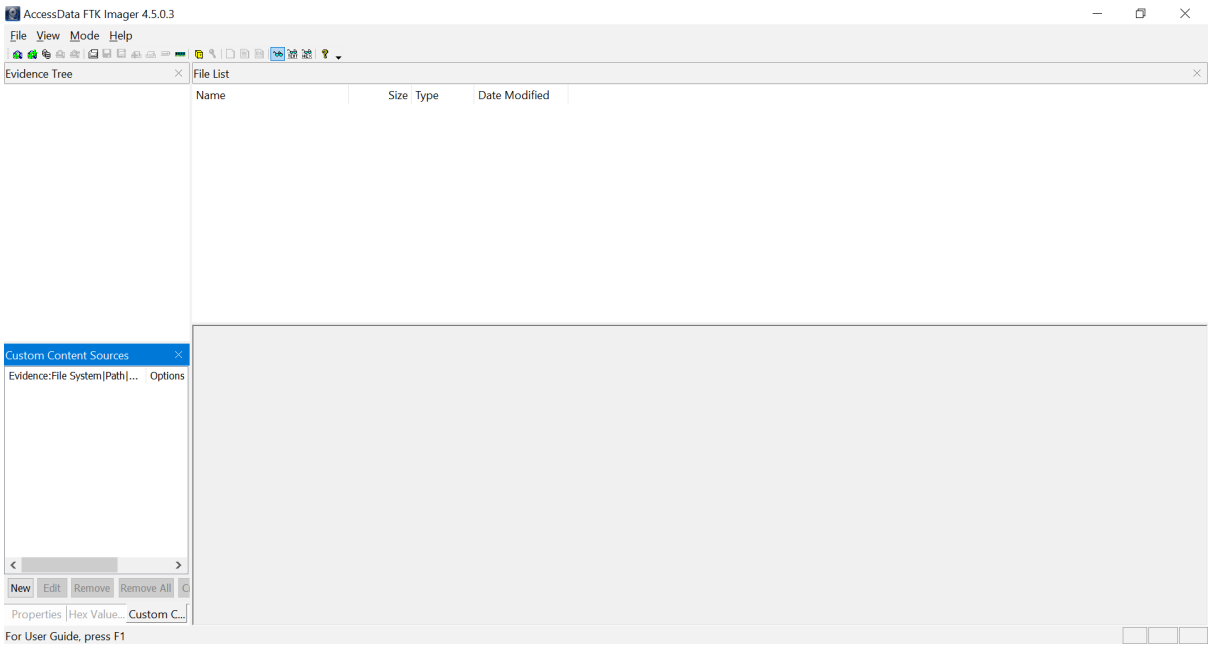


Figure 5: FTK Imager

VIEW MENU

The View menu allows you to customize the appearance of FTK Imager, including showing or hiding panes and control bars.

MODE MENU

The Mode menu lets you select the preview mode of the Viewer. Finally, the Help menu gives you access to help and information about FTK Imager.

HELP MENU

The Help menu provides access to the FTK Imager User Guide, and to information about the program version and so forth.

EVIDENCE TREE

The Evidence Tree (upper-left pane) displays added evidence items in a hierarchical tree. At the root of the tree are the selected evidence sources. Listed below each source are the folders and files it contains.

Click the plus sign next to a source or folder to expand the view to display its subfolders. Click the minus sign next to an expanded source or folder to hide its contents.

When you select an object in the Evidence Tree, its contents are displayed in the File List. The properties of the selected object, such as object type, location on the storage media, and size, are displayed in the Properties pane. Any data contained in the selected object is displayed in the Viewer pane.

Acquiring Evidence

What is a chain of custody?

How can we guarantee that evidence has not been modified?

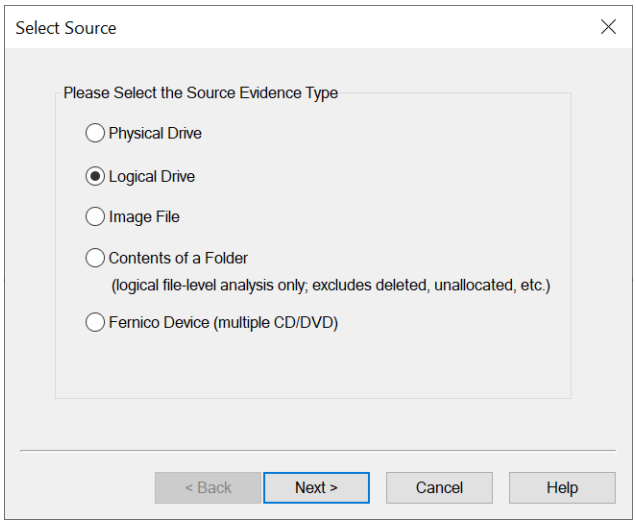
Logical Acquisition

What is meant by a logical acquisition?

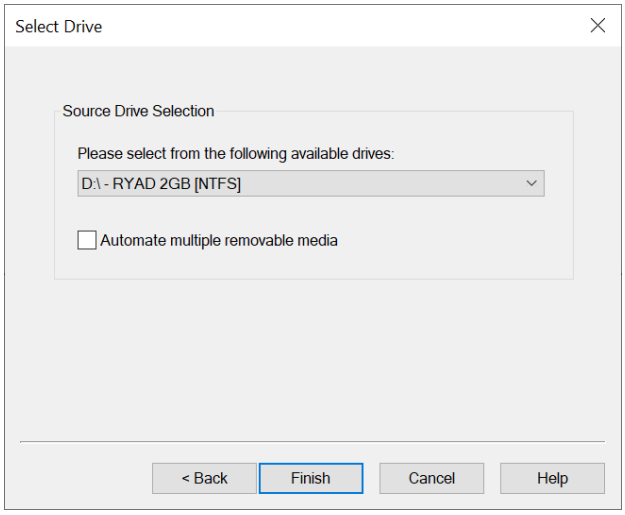
On your local machine, create a new folder called “lab2_FTK”.

Connect a USB-drive to the Windows machine. In FTK imager:

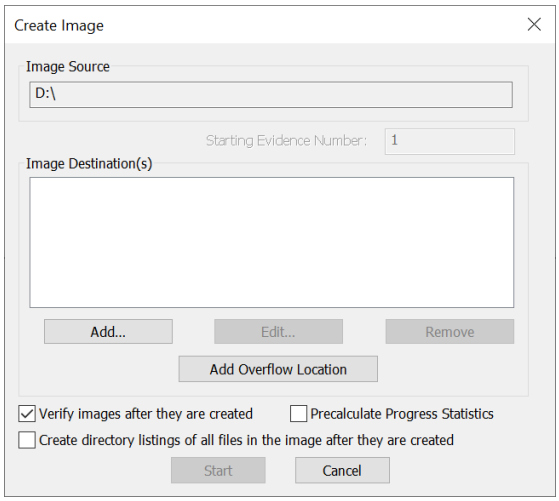
1. Click File > Create Disk Image
2. Select logical Drive and click “Next”



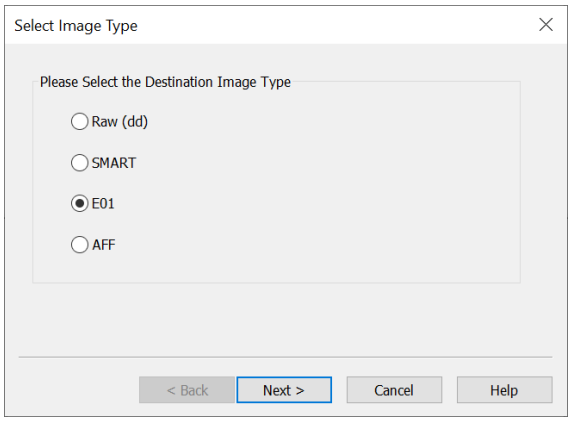
3. Select your USB drive and then “Finish”.



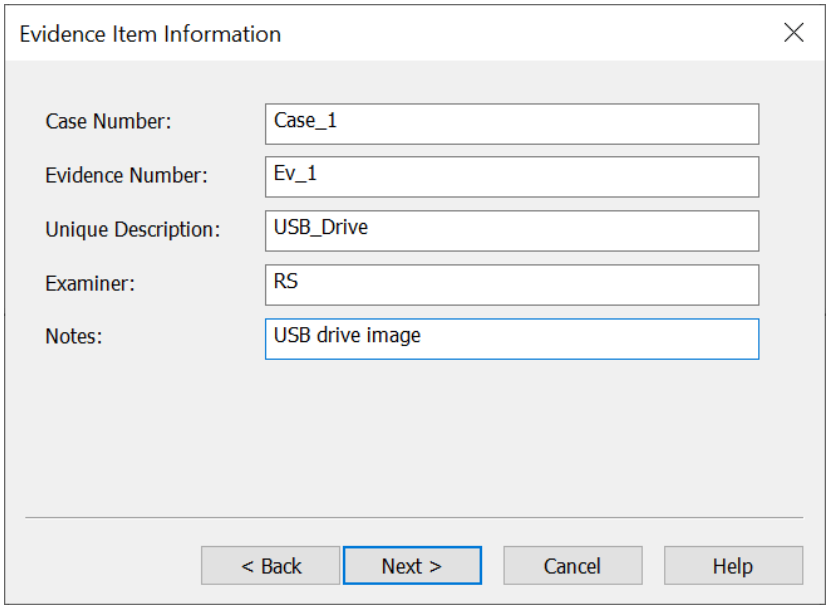
4. Add the destination for the image using the “Add” button.



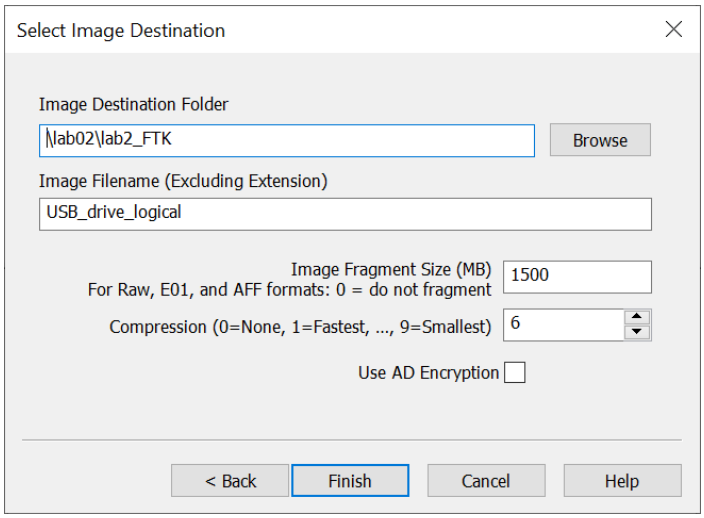
5. You will be asked for the image type. Try creating a E01 image and click next.



6. Add information for the evidence item and click next.

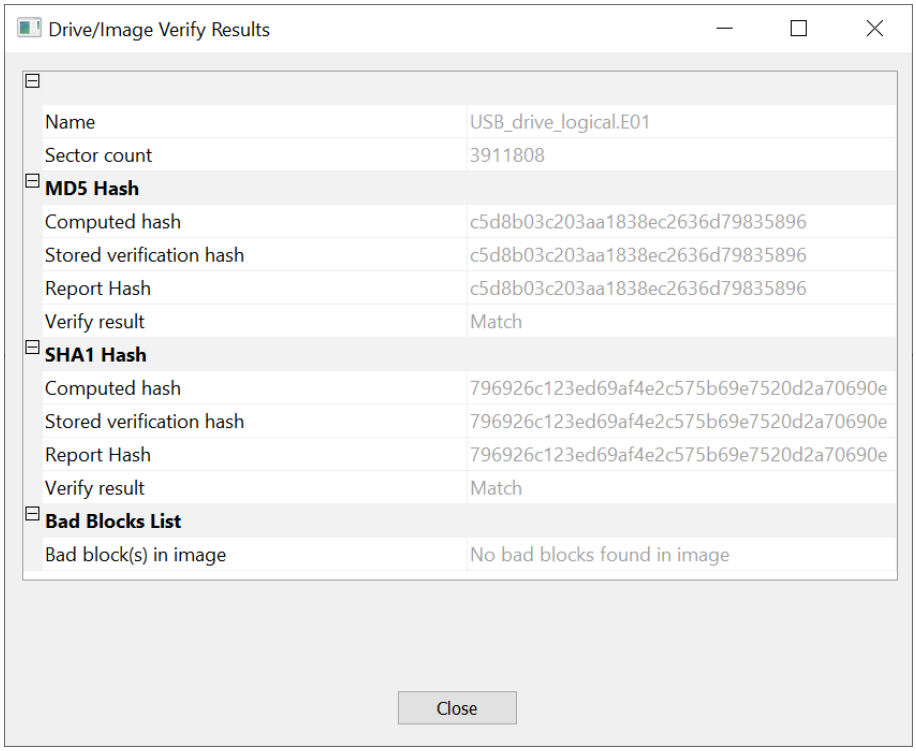


7. Browse to save the Image on the folder you created earlier (lab2_FTK folder) and name it "USB_drive_logical" and click finish.



8. And finally select "Start". Depending on the size of your USB drive, it might take sometime for the image to be created.

After the creation of the Image you will see a screen similar to the following snapshot:



What is MD5 and SHA1, and why are they important?

You can create a Physical Acquisition following the same steps, you need to choose “Physical Drive” in the select source window.

What is meant by physical acquisition? How is it different from logical acquisition?

Create a physical acquisition of the USB drive you used and upload a screenshot of the ‘Drive/Image Verify Results’.

A Case: Using FTK Imager – a Forensic Image of a USB key

Please copy file **usb_a.E01** (From Canvas, in “Resources” module)and save it in your local machine.

In FTK Imager click File > Add Evidence Item. Then choose image file and select next. Choose **usb_a.E01** and then add it as an Evidence Item, as can be seen in Figure 7.

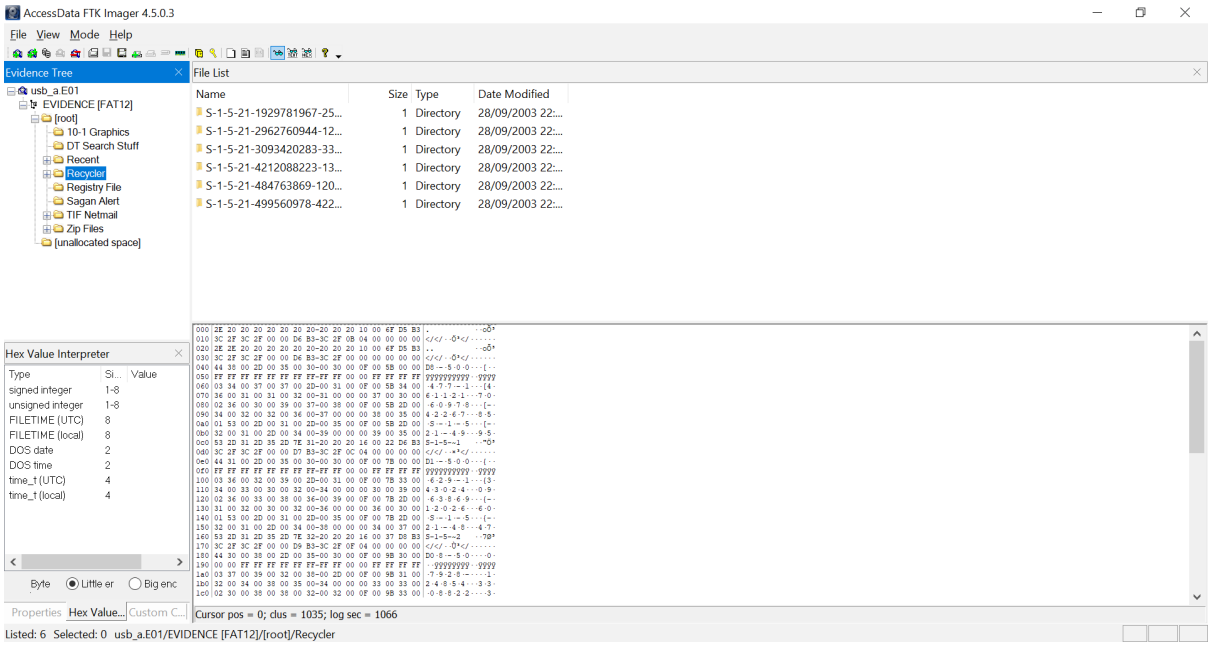


Figure 7: Evidence Items

Expand the Evidence Tree to find folder root/Recycler. Each folder within Recycler is a SID (security identifier) folder.

What is a SID folder?

How is the SID folder used by Microsoft operating systems? [Hint: Try searching in Microsoft Developer Network. There is also some information on other websites.]

The SID folders are in the Recycler folder. Search for a file called INFO2 in the SID folder whose name ends in 1004.

What did you find out about SID folders with names ending with a number like this (1004)?

What does a SID folder with a name ending in 500 indicate?

View the contents of INFO2 using the default viewer. Try looking at it in Text View. On the top pane choose the glass with Text under it.

Note that there is an INFO2 file in every SID folder but only one has any content. The INFO2 files lists the names of files in the Recycle bin and the names of any files which were in the Recycle bin which have been deleted or restored (**restored files have no drive letter**).

Give the name of a file that has been restored.

Under root, go to recent folder and identify .lnk files. These are Windows shortcuts.

In the folder TIF Netmail find the file index.dat, view it in text mode – you may prefer to export it and view it in Notepad.

This file contains browser usage information (cookies, history, TIF files).

Within the subfolders in the TIF Netmail folder there are a number of image files and .htm files. Click on these (ensure that the View Mode is Automatic, just the glass) 

.

You should see the content of the web pages or graphics files, as appropriate.

Can you match the content of index.dat with some of the images in the other folders? If yes, provide the filenames.

End of Lab Sheet