**Practical No. 1**

**File system Analysis using The Sleuth kit, Autopsy**

## How to Start a Case

## Upon starting Autopsy 3.1.2, a window will open with three selections to make: create a new case, open existing case, or to open a recent case.

Step 1) Select the “Create New Case” option and be directed to a new window that will have information to fill in, we will be naming the case “Test.”

Step 2) After the information has been filled in select the next button. The next window will allow the investigator to fill in the case number and examiner name. This is for the purpose of creating better documentation and logging. After the information is filled in select the finish button to continue.

Step 3) The next step in the investigation will be to add an image file to the case. The image file can be chosen from a wide variety of formats including: img, dd, 001, aa, and e01. Use the browse button to find the image that is desired to work with and select add. Options to choose the timezone of where the image came from as well as to ignore orphan files in FAT file systems are available to be selected based on the investigators preference and situation.

Step 4) After selecting the next button the image will be added to the case and the next button should be selected again if there are no errors.

Step 5) The following window will bring the investigator to the Ingest wizard panel, which is one of the new features offered in Autopsy. There are three options in the first box: Recent Activity, Hash lookup, and Keyword Searches.

By selecting any of the options advanced settings can be set to increase the capabilities of the search. Under the Hash Lookup option there is the advanced option to add databases of known hashes.

Under the Keyword Search option are many different lists that can be used to search for information. By default, Phone Numbers, IP Addresses, Email Addresses, and URL’s are available. Select the Advanced button and a Keyword List Configuration window will open. In this new window select New List and type the name that is desired for the list. This makes it easier to search by subject matter or other organizational methods. For now the list Test keywords will be used to create a list. In the adjacent pane there is a blank section with a word bar and an Add button next to it. Type the keyword desired (case sensitive) and select Add to add the word to the list. There is also the option to select Regular Expression.  This allows the investigator to further narrow the field to search in by selecting what the keyword is that is being searched for including: passwords, emails, text file name, domains, and many more options.

Step 6) After finishing the keyword parameters the screen will be laid out for the user.

Step 7) After the image is indexed the tree will be populated by the file system, extracted content, keyword searches, and the hash list (if any were used).

the investigator should generate a report. This will allow the investigator to have an idea of what type of information is available and what to expect. The report can be generated in three formats: Excel, XML, and HTML. It also has the ability to select what information to display with choices that can be seen in the image below.

Step 8) With the report on hand the investigator will have an idea of what to expect as well as a list of programs that are installed on the machine. This can help investigators gather all the evidence they need to perform a complete investigation.

Looking at the tree, the top selection is titled “Data Sources” this is where the acquired image is located and the bulk of the investigation, will take place. If the Images tab is expanded the investigator will see each image that was added to the investigation. By expanding an images tab the volumes of the image will be seen including the file system and unallocated space. Expanding the tab that contains the Operating System will give the investigator a look at the root directory and the tree that contains most of the relevant information. This is the same as if the investigator would open the default drive when browsing through a system.

Below the Images tab is the “Views” tab that will allow the investigator to separate the information in the image into different categories such as by file types and by recent documents. The file type can be broken down into: images, video, audio, and documents which includes the major text formats. Another section in the Views tab is a new feature in Autopsy 3, the Recent Files tab. This tab allows the investigator to get a rough outline of what happened in the last 6 days of use by the suspect. The results include registry files, documents opened, and programs run.

The next tab that is seen is the Results tab, this is a new feature that displays all the information from the ingest process. This uses the program BEViewer to look for certain information inside of the data and separate it into sections that make it easier to search for specific data instead of going through all of the information manually. Although this simplifies the investigation process, it does not mean that this is all of the information that is able to be gained through an investigation.

**Practical No: 02**

**Aim: Using Data Acquistion tools Exploring ProDiscover Basic.**

**Creating a New Project:**

Step 1) Start ProDiscover. ProDiscover presents the launch dialog.

Step 2) Enter a project number, project name, and description of the project in the new project tab

option, and then click the Open button.

ProDiscover will then create a project and generate a template report in the work area.

**2) Saving a project:**

1] Select save project option from the file menu, or button bar.

2] ProDiscover presents file Save As dialog if the current project has not yet been saved, otherwise the current project file will be updated without further action.

3] Select the destination path and click the **Save** button.

4] ProDiscover saves the project at the path specified.

**3)Preview a directly connected evidence drive**

1] Launch ProDiscover.

2] Select **open project** tab option.

3] Select the project file to open and click **Open** button.

4] ProDiscover opens the project file and generates a template report in the work area.

5] Select the **Add Disk** option from the action menu, or tree-view.

6] ProDiscover presents a dialog with all physical disk available for viewing.

7] ProDiscover then adds the physical disk to the currently active project.

8] Perform actions on the newly added disk such as search, hash compare and recovery).

**4) Conducting Live Preview of a Remote Disk (NOT DONE )**

**5) Capture an image of an attached drive**

1. Ensure the desired evidence drive is attached to the ProDiscover system.

2. Select the capture image option from the action menu item, or button bar.

3. ProDiscover presents the capture image dialog.

4. Select the drive to be captured, destination path for the image file to be saved into, compression

and password protection of the image file and specify the technician name, image number,

description of the image file.

5. We also have the option to select the desired image format. ProDiscover recommends using the ProDiscover format which includes adding metadata to the image containing information for password protection, time zone, investigator and compression. A technical description of the

ProDiscover image format can be found on the Technology Pathways web site in the resources section. Alternately, users can select to create an image in the UNIX style 'dd' format which creates a flat bit-stream image and a corresponding hash file using the selected hashing algorithm. the corresponding hash file will be placed in the image directory and named the same as the image using a .md5 or .sha file extension.

6. To compress the image select "Yes" to compression and ProDiscover will compress the image and save it as \*.cmp. Note that compressing an image requires more time to capture due to the compression overhead.

7. Click "OK".

8. ProDiscover reads the drive connected bit-by-bit and creates an image file in the specified

location. The image file will contain an exact replica of the original disk, plus a few bites of

checksum and log data.

9. ProDiscover will create a log file if there are any I/O errors.

**6) Capturing Physical Memory**

**7) Add an image file to a project:**

1. Launch ProDiscover.

2. Select **open project** tab option.

3. Select the project file to open and click **Open** button.

4. ProDiscover opens the project file and generates a template report in the work area.

5. Select the **Add Image** option from the action menu, or tree-view. Users may also right-click on "Disks", "Images" or "Remote Drives" from Content-view to add a disk, image or remote drive to the project.

6. ProDiscover presents the file open dialog.

7. Select the desired image file and Click **Open** button. If the image is of a Windows NTFS

Dynamic Disk, users should select the image's corresponding \*.pdg file which describes the disk group. If the image was a ProDiscover Split image, users should select the \*.pds file which describes all split files comprise the total disk image.

8. UNIX style "dd" images can be added to projects provided with or without the .eve file extension. To add a dd image to the project without an expected extension choose "All Files

(\*.\*) from the "File of Types" Drop down list. If the "dd" image is split into several images they should be numbered sequentially and all contain a .eve file extension. Once the image files are named and numbered correctly a corresponding \*.pds file should be created in the following

format:

DD-SplitImage

D:\Images\Splits\dd\Split0.eve

D:\Images\Splits\dd\Split1.eve

D:\Images\Splits\dd\Split2.eve

D:\Images\Splits\dd\Split3.eve

D:\Images\Splits\dd\Split4.eve

9. Note that all split image file should be split in sizes which are multiples of 512. To add the split

"dd" image users should select the split.pds file created above.

10. ProDiscover then adds the image file to the currently active project.

**8) Add a UNIX "dd" image file to a project**

To add a UNIX "dd" image:

1. Ensure your "dd" image has the file extension ".eve".

2. Launch ProDiscover.

3. Select **open project** tab option.

To Capture Unix ”dd” image:

Click on Proceed

3. Select the project file to open and click **Open** button.

4. ProDiscover opens the project file and generates a template report in the work area.

5. Select the **Add Image** option from the action menu, or tree-view. Users may also right-click on

"Disks", "Images" or "Remote Drives" from Content-view to add a disk, image or remote drive to the project.

6. Select the desired image file and Click **Open** button.

7. ProDiscover then adds the image file to the currently active project.

**9) Copy a directly connected drive to another directly connected drive**

1. Ensure the desired evidence drive is attached to the installed ProDiscover system.

2. Select the copy disk option from the action menu, or button bar.

3. Select the source and destination disk, then click **OK.**

4. ProDiscover copies the source disk to the destination disk.

**10) Restore an Image to directly connected drive**

1. Ensure the desired destination drive is attached to the installed ProDiscover system and its size will accommodate the original image.

2. Select the copy disk option from the tools menu, or button bar.

3. ProDiscover presents a dialog with the list of all local drives on the system.

4. Select "**Image**" from the source section of the dialog box.

5. Select the "**Browse**" button and locate the desired image. Note: Native ProDiscover images and

UNIX "dd" images can be restored.

6. Select the desired destination disk, and then click **OK.**

7. ProDiscover restores the image to the destination disk.

**11) Copy Selected Files**

In many cases you will want to recover items to another location in preparation for evidence presentation or further analysis. The "Copy Selected Files" option from the Tools Menu provides users with the ability to conduct a batch recovery/transfer of all items marked as "Evidence of Interest" by enabling the "Selected" Tag within "Content View".

**12) List detail information about image files associated with a project**

1. Select "**Content View | Images", or "Cluster View | Images**" from the tree-view.

2. ProDiscover lists detailed information of all image files associated with a project.

**13) View the contents of a directly connected disk as files**

1.Ensure the desired evidence disk is connected to the ProDiscover system and the desired disk has been added to the current project.

2. Select the "**Content View | Disks | Physical Drive | Partition**" option from the Menu or

tree-view. Note: Disk containing a Hardware Protected Area will display [HPA] after a partition to indicate any file systems detected within the HPA. See Advanced tips and tricks for more information on the HPA.

3. Select the desired disk partition.

4. ProDiscover displays the contents of the disk.

5. Select a file or directory to view from the work area.

6. ProDiscover displays the contents of that file at the bottom of the main window.

7. Double click on a file.

8. ProDiscover displays the contents of the file in the default file viewer. If no viewer has been set,

ProDiscover will launch an "**Open With**" dialog box asking the user to select an application to

open the file.

**14) View the contents of a disk, or image file as clusters**

1. Select "**Cluster View | Disks, or Image | Physical Drive | Partition**" from the View Menu or tree-view. Disk containing a Hardware Protected Area will display [HPA] after a partition to indicate any file systems detected within the HPA. for more information on the HPA.

2. ProDiscover presents a graphic representation of clusters for image file, or disk in the work area.

3. Select an individual cluster.

4. ProDiscover displays the contents of that cluster at the bottom of the main window.

**15) Viewing the Windows Event Logs (button disabled in demo version)**

**16) View Windows Registry**

**17) Search the Windows Registry**

**18) View Graphic Files in Gallery View**

In situations where users need to view the contents of a large number of graphic files in a given directory ProDiscover offers a "Gallery View" function. To shift into a gallery view mode users need only choose the "Gallery View" menu option from the "View" menu or right click over the work area as seen below.

Once the user selects "Gallery View" the work area view will display a thumbnail of all images within the selected directory as seen below.

**19) Adding Thumbnail Images to Report for Graphic Evidence**

Users may desire to add preview thumbnail images along with information provided to the standard

project report. To add graphic thumbnail preview images users should use the "Appearance" tab of the "Preferences" File menu option. In the appearance section users will find the following two options:

"**Add thumbnail image to report for graphic files**" (default unchecked) when checked will cause a

thumbnail image to be created and added to the report for any graphic file which is selected as evidence

of interest. For users who choose this option after graphic files have been added as evidence of interest they can use the Action menu's "Create report thumbnails" option to add thumbnails to the report.

"**Create thumbnails on load**" (default unchecked) when checked causes ProDiscover to automatically add thumbnail images to the report when opened. Warning: a large report, with many graphic files selected as evidence of interest, can cause a significant delay while loading a project file.

After choosing the desired settings thumbnail images will be added to the live ProDiscover project report (as seen below) as well as any report that is exported in the RTF format.

**20) View Image EXIF Meta Data**

Step 1) To view the EXIF meta data of a JPG or TIF file in ProDiscover simply right-click on any .jpg or .tif graphic file from content-view and select "View EXIF data" as seen below.

Step 2) After choosing to view EXIF Data, users are shown a dialog box containing all available EXIF meta data as seen below.

In the user preferences "EXIF" tab, users have the ability to select if they want EXIF meta data added to the report when selecting (selected tag enabled) graphics files as evidence.

**21) Recover a Deleted File**

1. Ensure the desired evidence disk is connected to the ProDiscover system.

2. Select the "**Content View | Disk, or Image**" option from the Menu or tree-view.

3. ProDiscover displays a list of drives, or images available to the system.

4. Select the desired disk, or image and navigate to the desired volume.

5. ProDiscover displays the contents of the disk.

6. Select a file to recover from the work area.

Notes: The "Deleted" column will display "Yes" if the file has been deleted. On NTFS formatted drives, ProDiscover collects all deleted files into a special directory called "Deleted Files". The contents of a recovered file can never be guaranteed since some clusters may have been overwritten.

7. ProDiscover displays the contents of the selected file at the bottom of the main window. **Right click** on a file.

8. In ProDiscover a pop-up dialog with the choice to View or Recover the selected file. Select **Copy**

**File.**

9. Enter the desired location and file name to save the file as in the "Save As" dialog box that

appears and click "**Save**".

**22) Search for keywords in image file or disk**

Step 1) From the current project select search option from the tree-view, or button bar. ProDiscover displays search dialog.

Step 2) Choose the type of search to be conducted (Content or Cluster).

Step 3).If conducting a content search choose "Search in Selected Files only" to search in only files selected as evidence if desired.

Step 4).Checking the "Select all matches" checkbox will automatically add all files from the search result to the project report as evidence of interest. Files marked as evidence of interest can be easily copied to review disks using the "copy selected files" option from the tools menu.

Step 5) If conducting a content search choose to search for file names or content.

Step 6) Enter the keywords (one on each line) in the search for window and select the image files or disks to be searched. Full Boolean Logic (AND, OR, NOT) can be used, but must be capitalized.

List of keywords can be saved in an ASCII text file with the extension .STS and loaded using the "Load from file..." button.

Step 7) Users may also select to filter Content Searches by Modified, Accessed, or Created dates.

Step 8) Click the "Search Now" button.

Step 9) Results obtained from the search will be displayed in the top work area as selectable objects.

When any object is highlighted the resulting search term will be highlighted in the data view area.

Search results are saved from session to session in a file with the same project name and the extension .ds2

Step 10) If the search results are satisfactory they can be added to the current projects report with the "Add to Report" button.

Step 11) The "Search terms" drop-down box allows users to highlight only a single search term from the original search term list if desired.

Step 12) The "Patterns" button will display a pop-up window containing the original search terms used in the search set including any Boolean operators used.

**23) Extracting Internet History**

Information about a users Internet Web surfing habits is often crucial to investigations. ProDiscover allows investigators to quickly search for, and extract information from Internet Explorer history files (index.dat). Once the information is extracted it is automatically added to the project report.

Step 1) Searching for and extracting the Internet history from a directly added disk or image is as simple as rightclicking on the desired directory structure and choosing "Find Internet Activity...".

Step 2) Once complete the Internet History Viewer found in the tree-view will be populated with the contents of each index.dat file created by Internet Explorer. Once added to the Internet History Viewer this information can be searched and added to the project report on an entry-by-entry basis.

**Practical No: 03**

**Using File recovery Tools**

**Aim: Understanding & working with the process of the process of taking a drive image using AccessData's FTK Imager tool.**

Step 1) Run **FTK Imager.exe** to start the tool.

Step 2) To create a forensic image:

Click File > Create Disk Image

Step 3) In the Select Source dialog box, select the source you want to make an image of. Click Next.

If you select Logical Drive and need to select a floppy or CD as a source, you can check the Automate multiple removable media box to create groups of images. Imager will automatically increment the case numbers with each image, and if something interrupts the process, you may assign case number manually.

Step 4) Select the drive or browse to the source of the image you want, and then click Finish.

Step 5) In the Create Image dialog, click Add.**...** to add the image destination.

* Compare the stored hashes of your image content by checking the Verify images after they are created box. If a file doesn’t have a hash, this option will generate one.

List the entire contents of your images with path, creation dates, whether files were deleted, and other metadata. The list is saved in tab-separated value (.TSV) format.

Step 6) Select the type of image you want to create.

The type you choose will usually depend on what tools you plan to use on the image. The dd format will work with more open source tools, but you might want SMART or E01 if you will primarily be working with ASR Expert Witness or EnCase, respectively.

Note: If you are creating an image of a CD or DVD, this step is skipped because all CD/DVD images are created in the IsoBuster CUE format. Hashes are not generated for CD and DVD images so they will not be verified, as well.

Important: The raw image type is not compressed. If you select the Raw (dd) type, be sure to have adequate available drive space for the resulting image.

Step 7) If you are creating an AFF image type, choose AFF. Click Next.

The Image Destination Folder dialog box you see will be different than that seen when selecting any other image type

Step 8) If your version of FTK requests evidence information, you can provide it. Specify Evidence Item Information. All Evidence Item Information is optional, but it is helpful to have the information easily accessible in case it is called into question at any time after creation

Complete the fields in the Evidence Item Information dialog. Click Next.

Step 9) Select the Image Destination folder and file name. You can also set the maximum fragment size of image split files. Click Finish to complete the wizard.

In the Image Destination Folder field, do one of the following:

* Type the location path where you want to save the image file.
* Click Browse to find and select the desired location.

In the Image Filename field, specify a name for the image file but do not specify a file extension.

Step 10) Specify the Image fragment Size:

* Default Image Fragment Size = 1500 MB
* To save images segments that can be burned to a CD, specify 650 MB.
* To save image segments that can be burned to a DVD, specify 4000 MB.
* The .S01 format is limited by design to sizes between 1 MB and 2047 MB (2 GB). Compressed block pointers are 31-bit numbers (the high bit is a compressed flag), which limits the size of any one segment to two gigabytes.

Step 10 a) Select the compression level to use.

* 0=No Compression
* 1=Fastest, Least Compression (faster, and also slightly smaller than a 0-compression file)
* 9=Slowest, Most Compression (smallest file, slowest to create).

Numbers between 1 and 9 produce an image with varying levels of compression to speed ratio.

Step 11) To encrypt the image, choose the correct encryption box as explained below:

a. To encrypt the new image with AD Encryption, mark the Use AD Encryption box.

b. To encrypt the new image with AFF Encryption, mark the Use AFF Encryption box.

Step 12) Click Finish.

Step 13) When AFF Encryption is selected, type the password, and retype the password to confirm. Click Show Password to see that you have typed it correctly the first time.

Step 14) When encryption selections are made, click **OK** to save selections and return to the **Create Image dialog.** Click **Start** to begin the imaging process.

After the images are successfully created, the Drive/Image Verify Results box shows detailed image information, including MD5 and SHA1 check sums, and bad sectors.

Now is a good time to refill that coffee cup! Once the acquisition is complete, you can view an image summary and the drive will appear in the evidence list in the left hand side of the main FTK Imager window. You can right-click on the drive name to Verify the Image:

A progress dialog appears that shows the following:

* The source that is being imaged
* The location where the image is being saved
* The status of the imaging process
* A graphical progress bar
* The amount of data in MB that has been copied and the total amount to be copied
* Elapsed time since the imaging process began
* Estimated time remaining until the process is complete
* Image Summary button. Click it to open the Image Summary window as shown below:

**Practical No: 04**

**Using Steganography tools**

**Aim: Exploring S tools**

Following steps Show how to use freeware S-Tools utility to hide and reveal files inside pictures

Step 1) Select the S-Tools.exe file and open the steganography software tool.

Step 2) With both the working directory and the S-Tools program open minimize both windows and place side-by-side.

The S-Tools program is a drag and drop software. The files used to create the steganography file can be dragged from the directory into the S-Tools program.

Step 3) Select the file from the directory and drag it over the S-Tools main window and release the

file.

A dialogue box appears indicating that the file type is unknown. Supported file types for audio and image files are shown below:

* Audio - \*.wav
* Image - \*.bmp and \*.gif

If your image is in .jpg format, convert it to .bmp format by doing the following steps using Paint:

Step 4) Select a valid audio file or image as the base file for the steganography file. The Tulips.bmp was selected and dragged onto the main window of the S-Tools program. The image is opened.

Step 5) Select a file to hide within the base file. If it’s not there, create a txt file and Save the file.

Step 6) The \*.txt text file is selected and dragged on top of the base image. Release the file while the cursor is still on top of the base file.

Step 7) A dialogue box will appear asking the user to enter and verify a passphrase. Additionally, the user will have to select an encryption algorithm.

Step 8) Enter a passphrase in both the passphrase and verify passphrase text boxes. If the same passphrase is not entered in both text boxes the ‘OK’ button will be grayed out and the

user will not be able to proceed to creating the steganography file.

Step 9) Select the ‘OK’ button after entering a valid passphrase.

Step 10) The S-Tools main window will appear and a new file will be visible. The name of the file will be called hidden\_data by default.

Step 11) Place the cursor on top of the hidden data image and select the right mouse button. The user will

have four options available to them:

* Save
* Save As
* Properties
* Reveal

Step 12) Selecting the ‘Properties’ button while the cursor is over any image will display the following

properties:

* Width and Height of the image
* Bits per pixel
* Memory Usage (file size in bytes)
* Compression

Step 13) Selecting the ‘Reveal’ button will display a passphrase dialogue box. A passphrase must be entered twice in the dialogue box and the correct encryption algorithm must be selected.

Notice that the title of the dialogue box has changed to ‘Revealing from Tulips.bmp’

Step 14) Enter a passphrase twice, select the encryption algorithm, and select the ‘OK’ button.

Step 15) A ‘Revealed Archive’ dialogue box will display which contains the file name and size of the hidden file.

Step 16) Select the ‘Save As’ button.

Step 17) A ‘Save As’ dialogue box will appear. Enter a valid file name, select the working directory and select the ‘Save’ button.

Step 18) Locate the files in the working directory.

Step 19) Open the files using a multimedia software program and ensure that the files were extracted from the steganography file successfully.

**Practical No: 05**

**Using Accessdata FTK**

**Aim: Exploring Access data FTK for the following:**

**Data Carving**

Searching for Embedded and Deleted Files (Data Carving)

Because embedded items and deleted files contain information that may be helpful in forensic investigations, Forensic Toolkit (FTK) simplifies the process of recovering these items and adding them to the case. The data carving feature allows you to search for items, such as graphics embedded in other files. It also allows you to recover previously deleted files located in unallocated space. To recover embedded or deleted files, FTK searches the index for specific file headers. When it finds a file header for a recognized file type, FTK carves the file’s associated data. FTK can find any embedded or deleted item as long as the file header still exists.

Data carving can be done either during **evidence processing (when a new case is added)** or it can be done in **an existing case.**

**Data Carving Files During Evidence Processing in a New Case:**

You can select to data carve when a case is added by selecting Data Carve in the Process to Perform Screen during the New Case Wizard. FTK carves data immediately after pre-processing.

When you select to data carve when creating a new case, FTK creates a cache for the carved data. If data is located, the cache is saved.

To access the cache:

1 Select **Tools**, and then **Data Carving**.

Step 2) Check the file types to carve. You can click **Select All** or **Select None** to speed up the selection process. Click **OK**.

When the process is complete, the detached viewer appears with the data carving results. A message appears if no data was located.

**Or**

**Data Carving Files in an Existing Case:**

To search for embedded and deleted files:

1. Select **Tools**, and then **Data Carving**.

[2] Check the file types to carve. You can click **Select All** or **Select None** to speed up the selection process.

[3] (Optional) Check the **Automatically Add Carved Items to Case** option. The the Minimum Image Size fields activate. 3a Specify a minimum size in pixels in which to disply images. The program will question you about minimum sizes over 480 pixels.

[4] Click **OK**.

When the process is complete, the detached viewer appears with the data carving results.

**Adding Carved Files to the Case:**

To add a carved file to the case:

1. Select the files you want to add to the case.

You can Shift+click to select multiple contiguous files. or Ctrl+click to select multiple discontiguous files.

1. Click **Add Items to Case**.
2. Click **Yes** to accept the default name. or Click **No**, enter a different name, and click **OK**.

After a file is added to a case, FTK will not find it in subsequent data carving procedures. In other words, there is no redundancy. If a file is identified as case evidence, the data carving feature ignores it. The data carving feature only looks for files that are not individually identified in the body of evidence.

**Bookmarking Carved Files:**

To bookmark a carved file:

Step 1.Select the files you want to include in the bookmark and click **Create Bookmark**.

Step 2.In the Create New Bookmark form

Step 3. Enter the following & Click **OK**.

When the process is complete, the detached viewer appears with the bookmarked data carving results

**Using Filters**

**Applying an Existing Filter**

To apply an existing filter, use the Filter drop-down list on the File List toolbar, shown below:

**Using the File Filter Manager:**

The File Filter Manager allows you to create or modify file filters.

To access this menu, select **View**, and then **File Filter Manager**

he following sections review the categories in the File Filter Manager menu:

**Modifying or Creating a Filter**

To modify or create a filter:

Step 1. Select **View**, and then **File Filter Manager**.

Step 2.Select the filter that you want to modify.

Step 3.If you are modifying an existing filter, click **Save/Apply**. Or

If you are creating a new filter, click **Save As**, enter the name, and click **OK**.

**Deleting a Filter**

You can delete a filter if you no longer need it. To delete a filter:

Step 1.Select **View**, and then **File Filter Manager**.

Step 2.In the **Selected Filter** drop-down list, select the filter that you want to delete.

Step 3.Click **Delete**.

**Searching the Registry**

**Launching Registry Viewer as a Separate Application:**

To run Registry Viewer as a separate application, select **Start**, then **Programs**, then **AccessData**, and then **Registry Viewer**, and then **Registry Viewer**.

**Launching Registry Viewer from FTK:**

To run Registry Viewer from FTK:

Step 1.In FTK, open an existing case by selecting **File**, and then **Open Case**.

Or if you have chosen to always display the FTK Startup screen, select **Open an Existing Case** and click **OK**.

Step 2.Select the case you want to open.

Step 3. Select **File**, and then **Registry Viewer** to open Registry Viewer.

(Can’t perform ahead of this step because Registry viewer is disabled in demo version)

**Obtaining Protected Registry Files Using FTK Imager**

To obtain the protected registry files using FTK Imager:

Step 1. Launch FTK Imager.

Step 2.Click **File**, and then **Obtain Protected Files**

Step 3.Designate a destination directory and file options, then click **OK**.

FTK Imager exports the selected files to the designated location.

Add the files to the case in FTK.

**Generating a Report**

To generate a report file,

1. From the menu, select **Report**, and then **Generate Report** or click the button on the toolbar.

2. The Case Information dialog appears.

3. The Bookmarks-A dialog appears.

4.The Bookmarks-B dialog appears

5. The Graphics Thumbnail dialog appears

6. The List by File Path dialog appears

7. Then List File Properties-A dialog appears

8.The Create Report dialog appears. In the Report Title field, enter a name for the report file. In the Report Location field, enter the location where you want to save the report file or click **Browse** to navigate to the desired location.

**Practical No: 06**

**Using Log Capturing and Analysis tools**

**Aim: Exploring Wireshark**

Wireshark is a network packet analyzer that intercepts, captures and logs information about packets passing through a network interface. This is useful for analyzing network problems, detecting network intrusions, network misuse, and other security problems, monitor usage and gather statistics, and many other applications.

### Filtering Packets

If you’re trying to inspect something specific, such as the traffic a program sends when phoning home, it helps to close down all other applications using the network so you can narrow down the traffic. Still, you’ll likely have a large amount of packets to sift through. That’s where Wireshark’s filters come in.

The most basic way to apply a filter is by typing it into the filter box at the top of the window and clicking Apply (or pressing Enter). For example, type “dns” and you’ll see only DNS packets. When you start typing, Wireshark will help you autocomplete your filter.

You can also click the Analyze menu and select Display Filters to create a new filter.

Another interesting thing you can do is right-click a packet and select Follow TCP Stream.

You’ll see the full conversation between the client and the server.

Close the window and you’ll find a filter has been applied automatically — Wireshark is showing you the packets that make up the conversation.

Inspecting Packets

Click a packet to select it and you can dig down to view its details.

You can also create filters from here — just right-click one of the details and use the Apply as Filter submenu to create a filter based on it.

**Practical No: 07**

**Using Traffic Capturing and Analysis tools**

**Aim: Exploring Wireshark**

**Step 2**: On menu bar select Capture. Select interfaces.

**Step 3:** Select Once you click on start, then Wireshark starts to capture the packets on that interface.

**Step 4**: Filter packets with HTTP protocol.

**Step 5:** A file with only text: <http://www.mu.ac.in/ppe/LIBRARY%20SCIENCE-(SEM.I)-SH-2014.pdf>

**Step 6**: Applying different filters using expressions.

1) Filtering HTTP POST request

2) Filtering 404 not found error

3) Filtering using HTTP Content Length

**Practical No: 08**

**Aim: Exploring Mobiledit Forensics**

Mobiledit is a forensics software tool containing a built-in writeblocker. It can connect to phones directly via Bluetooth, and can read SIM cards by using a SIM reader. It’s also notable for being very user friendly. Steps:

1) Run MOBILedit1 Forensic Lite

2) Connect your mobile device . Click on Connect. Select Cable Connnectors

3) Eter password

3) Data will be acquired, as shown in the image below : Keep on clicking next

5) Select HEX Dump then Physical Analysis

6) We can retrieve call logs, messages, mms, e-mails, files, calendar, tasks, notes and other applications installed on the mobile device information

**Practical No: 09**

**Aim: Generating report Using AccessData FTK.**

First we need to **Create a Case:**

Step 1 :To provide the new case information: 1 In the **Investigator Name** field, type the name of the investigator. The drop-down list contains the name of investigators that have been entered in prior cases. If the investigator has worked on other cases in FTK, select the name from the list.

2 In the **Case Number** field, enter the case number for reference.

3 In the **Case Name** field, enter the name of the case. The name cannot contain the following characters: “ > ? / : \ | < The case name also becomes the name of the folder where all case information will be stored.

4 Next to the **Case Path** field, click **Browse** to select the path where the evidence will be stored. By default, all FTK cases are stored in that directory.

5 Verify that the **Case Folder** field lists the folder where you want the case to be stored. Each case is stored in a separate folder and should be kept distinct from other cases. The **Case Folder** field is based on the **Case Name** and **Case Path** fields. To make changes to the **Case Folder**, change the **Case Name** and **Case Path** fields.

6 (Optional) In the **Case Description** field, add information that will be helpful to the analysis of the case. This field is particularly useful if several people work on the case. This field is included in the report created at the end of the case investigation. Click **Next**.

**Entering Forensic Examiner Information:**

**Selecting Case Log Options:**

The Case Log Options form allows you to select which events you want FTK to log for the current case. FTK maintains a log file of FTK events such as bookmarking items, searches, and error messages for each case.

**Selecting Evidence Processes:**

The Evidence Processing Options form allows you to select which processes you want to perform on the current evidence. You only need to select those processes that are relevant to the evidence you are adding to the case. For example, if your case is primarily a graphics case, there is no need to index the evidence.

**Refining the Case:**

**Refining the Index:**

The Refine Index form allows you to specify types of data that you do not want to index. You might choose to exclude data to save time and resources and to increase searching efficiency.

**Managing Evidence :**

As your investigation progresses, you will want to edit the information you entered for your evidence. Evidence is managed through the Add Evidence forms.

**Reviewing Case Summary:**

The Case Summary form allows you to review the evidence directory, number of evidence items, and evidence processes that you selected during the New Case Wizard.

**Processing the Evidence :**

After you click Finish, the Processing Files form appears and displays the status of the processes you selected in the wizard.

1. From the menu, select **Report**, and then **Generate Report** or click the button on the toolbar.

2.The Case Information dialog appears.

3. The Bookmarks-A dialog appears.

4. The Bookmarks-B dialog appears

**Practical No: 10**

**Aim: Password Cracking Using Cain and Abel.**

Step 1 : Install and open cain and abel.

Step 2 : Select sniffer on the top.

|  |  |
| --- | --- |
| Step 3 : Next to folder icon click on icon name start/stop sniffer. | Select device and click on ok. |

Step 4 : Click on “+” icon on the top. Click on ok.

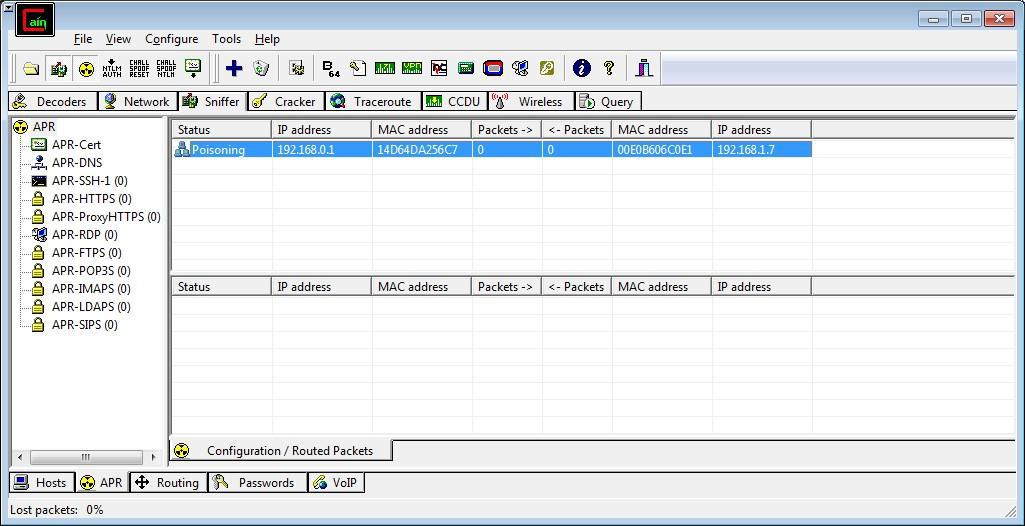
Step 5 : Shows the Connected host.

Step 6 : Select Arp at bottom.

Step 7 : Click on “+” icon at the top.

Step 8 : Click on start/stop ARP icon on top.

Step 9 : Poisoning the source.



Step 10 : Go to any website on source ip address.

|  |  |
| --- | --- |
| Step 11 : Go to password option in the cain & abel and see the visited | site password. |

**Practical No: 11**

**Aim: Using Windows Forensics Tools accessdata ftk**

Step 1: Start Forensic Toolkit.

Step 2: Here, prompted with a warning dialog box, click on OK to continue.

Step 3: click on OK button.

Step 4: Now select Start New Case option and click on ok.

Step 5: Enter the detail for a New case.

Step 6: Fill the information in Forensic Examiner Information dialog box.

Step 7: leave the default settings and click on next.

Step 8: Now again leave the default settings and click on next.

Step 9: In the Refine Case-Default, click the Include All items button and then click Next.

Step 10: In Refine Index-Default, accept the default settings and click Next.

Step 11: Now here Click on add Evidence button.

Step 12: Enter Evidence Information and click on OK button.

Step 13: Now click on Next.

Step 14: Click on Finish to initiate the analysis.

Step 15: Now Processing Will Start........

Step 16: when FTK finishes the processing part, the FTK window opens to the Overview tab.

Step 17: Select Deleted Files option to explore the evidence items.

Step 18: Select Encrypted Files to view.

**Practical No: 12**

**Aim: Using Email Forensics Tools using accessdata ftk**

For this practical we need to have .pst(personal storage table) file we need to configure our email using Microsoft outlook so that we can use .pst file as evidence for our case. we can configure our mail manually and automatically using outlook

**Step 1: Enable POP in your gmail account**

Login to your email account. Go to **Settings**, click on **Forwarding and POP/IMAP** tab

In **POP Download** section select the **“Enable POP for mail that arrives from now on”** option

Then click on the **“Save Changes”** button at the bottom of the screen

**Step 2: Enabling app settings**

To do so just copy paste the following url in the address bar of your browser (See that you are still logged into your account)

https://www.google.com/settings/security/lesssecureapps

In this page for the setting **Access for less secure apps** select the **“Turn on”** option.

**Step 3: Configure MS outlook by providing the required credentials**

Launch the **MS Outlook** from the **Start** button. At the **Outlook Startup** welcome screen click on **“Next”** button.

In the next screen it asks whether you want to configure an E-mail account… select **“Yes”** (default) and click on **“Next”** button

In the next screen it asks for the **E-mail account** credentials. Enter the credentials of your email account (for which you **previously activated POP feature**)

Check the “**Manually configure server settings or additional server types”** option at the bottom of this screen. Click on **“Next”** button.

Choose the **E-mail Service** as **“Internet E-mail”** and click on **“Next”** button.In the **Internet E-mail Settings** screen enter the details (as shown in the below right image). Click on **“More Settings…”** button (opens **Internet E-mail Settings** window).

In **Internet E-mail Settings** window go to **Advanced** tab and enter the credentials (as shown in below image). Then click on **“OK”** button.

In the below screen (below left image) click on the **“Test Account Settings…”** button.

In the **Test Account Settings** window it shows two **tasks completed successfully**. Click on **“Close”.**

Click on **“Finish”** button.

Now open Forensic toolkit and create case and add .pst file as evidence

Creation of case

Add necessary details

click on Next

click on next

now click on ADD Evidence to add .pst file

select individual file

Now Go back to outlook to copy the path where the .pst file is stored so that we can give that path in ftk to add .pst file to our case

Go to tools—Account settings

Go to data files—click on open folder

A window will be opened where the .pst file is stored

now copy the location

After copying the location Go back to FTK and paste that location in the file name field and click on open

select the outlook.pst file

give evidence number and click on OK

click on Next

click on finish

now you can see the .pst file is added to the FTK

go to email tabs and open the files you want

**Practical No: 13**

**Aim: Forensic Investigation Using Encase**

**Step 1**: Open the Encase software tool

**Step 2:** Click on New and enter the name and click on Finish.

**Step 3:** Check the left pane

**Step 4:** Click on Add Device and select “Local Drives” and click Next.

**Step 5:** Choose a device and click Next.(Choose NTFS)

**Step 6:** we can see the preview of the selected device and click Finish.

**Step 7:** We can see the device selected.

**Step 8:** Click on Edit and select Acquire.

**Step 9:** Click Next.

**Step 10:** Enter the Name and check the output path and click Finish.

**Step 11:** Acquiring process starts.

**Step 12:** Click OK.

**Step 13:** Verification result

**Step 14:** Select bookmark option, select “Logs”

**Step 15:** For viewing report, right click on Report tab and select Export.

**Step 16:** Click OK

**Step 17:** Open the file “export1.txt

**Practical No: 14**

**Aim: Using Wireless Forensics Tools using cain and abel**

**Step 1**: It displays the hosts with the ip address.

**Step 2:** Click on start/stop APR option and click on Add button (+).

**Step 3:** It displays the range of IP address. Select “All Tests”. Click OK.

**Step 4:** The test are run. All IP address in the range are shown.

**Step 5:** Goto the wireless tab select second option in dropdown and click on active scan button

**Step 6:** It shows the nearest wireless connection.

**Step 7**: Go to decoder tab and select wireless passwords.

**Step 8:** It shows the wireless connection and password.