# Practical No: 01

**Title:** Using Windows Forensics Toolkit

**Tools Used:** AccessData FTK

## Tasks to be performed:

- **Starting a new case**
  - Start the AccessData FTK. From **File** menu➔Select **New Case.**
    **or**
    In case you are opening the FTK for the first time, **FTK Start up Screen** is displayed ➔ Select **Start a New Case** option ➔ Click **OK.**
  - **Enter basic case information.**
    - The New Case form provides fields for basic case information, such as the case name and its investigator.
      - In the **Investigator Name** field, type the name of the investigator.
      - In the **Case Number** field, enter the case number for references.
      - 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.
      - 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.
      - 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.
      - 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.
      - Click on **Next**

  - **Entering Forensic Examiner Information**
    - The Forensic Examiner Information form allows you to enter information about the forensic examiner.
      - In the **Agency/Company** field, type the name of the agency or company.
      - In the **Examiner's Name** field, type the name of the examiner.
      - In the **Address** field, enter the address for the agency/company.

- In the **Phone** field, enter the phone number for the agency/company.
- In the **E-Mail** field, enter the examiner's e-mail address.
- In the **Comments** field, enter any necessary comments.
- Click on **Next**

- **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.
  - In the **Case Log Options form**,
    - Select what you want to include in the case log.
    - Click **Next**.

- **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.
  - In the **Evidence Processing Options form**:
    - Select the processes that you want to be run on the evidence.
    - Click **Next**.

- **Refining the Case**
  - The Refine Case form allows you to exclude certain kinds of data from the case.
  - FTK contains five default exclusion templates:
    - Include All Items
    - Optimal Settings
    - Email Emphasis
    - Text Emphasis
    - Graphics Emphasis
  - In the **Refine Case form**:
    - Select the default template that you want to use.
    - To modify the default options:
      - Select which items you want to unconditionally add to the case.
      - From the drop-down list, indicate whether you want to add items that satisfy BOTH the File Status and File Type criteria or items that satisfy EITHER the File Status or File Type criteria.
      - Select the **File Status criteria**.
      - Select the **File Type criteria**.

- Click **Next**.

- **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.
  - To modify the default index settings in the Refine Index form:
    - Select the types of files that you want to index.
      - Select which items you want to unconditionally index.
      - From the drop-down list, indicate whether you want to index items that satisfy boththe File Status and File Type criteria and items that satisfy eitherthe File Status or File Type criteria.
      - Select the **File Status criteria**.
      - Select the **File Type criteria**.
    - Click **Next**.

- **Adding Evidence**
  - Evidence is managed through the Add Evidence forms.
  - The Add Evidence form allows you to perform the following functions:
    - Add evidence.
    - Remove evidence.
    - Edit basic information about the evidence.
    - Create parameters for adding evidence to the case.
  - To add evidence to the case:
    - In the Add Evidence Case form, click **Add Evidence**.
    - Select **Acquired Image of the Drive** of the following evidence types and click **Continue**
    - **Browse** to Desktop and select the **precious.img** file. If you add an unidentified evidence item that is larger than 25 MB, it will be chunked into 25 MB pieces.
    - In the Evidence Information form, enter the following information and click **OK**:
      - Comment
      - Evidence Display Name
      - Evidence Identification Name/Number
      - Evidence Location
      - Local Evidence Time
      - Zone

- **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
- If you want to change or review any selections, click **Back** to return to the appropriate form. After you make your changes, click **Next** to return to the Case Summary form.
- To accept the current settings and start the processing of the evidence, click **Finish**.

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

## • Processing Evidences

- **Viewing file properties:**
  - To view a file's properties:
    - Highlight a file in the File List.
    - Select **Tools**, and then **File Properties**.
  - The File Properties menu is organized into five information windows:
    - General Info
    - File Source Info
    - File Content Info
    - Case-specific Info
    - E-mail Info (appears only when viewing file properties for email messages and attachments)
- **Using Bookmarks**
  - **Create a Bookmark**:
    - In a file list, highlight the file that you want to add to the bookmark.
    - Right-click and select**Create Bookmark**
    - **Create New Bookmark** wizard will be displayed.
      - In **Bookmark Name** field, type the bookmark name.
      - In the **Bookmark Comment** field, enter comments about the bookmark or its contents.
      - Check **Include in Report** to include the bookmark in the report.
      - Check **Export** to export the bookmark's files with the report.
      - Click **OK**.
    - To view the bookmarked files, click on the **Bookmark** tab.

- **Searching a case**
  - Searching evidence for information pertaining to a case can be one of the most crucial steps in the examination. Forensic Toolkit (FTK) provides both live and indexed searches.
    - Click on **Search** tab ➔ click on **Indexed Search**
    - In the **Search Term** field, enter the term you want to search for, including any wildcard characters. As you type your search term in the field, the Indexed Words list scrolls to match the term. The Count column displays the number of times each indexed word is found in the case.
    - Click **Add** to add the search term to the search list.
    - In the **Search Items** column, select the index term you want to search.
    - Click **View Item Results**to initiate the search. The Filter Search Hits dialog appears.
    - In the **Filter Search Hits** dialog, select **All Files**
    - Click **OK**

- **Working with Existing cases**
  - Start **AccessData FTK**➔ Click on **File** menu ➔ Select **Open an Existing Case**
  - Click **OK**to browse to the new location, and then choose the case file.
  - Click **Yes.** The FTK program will automatically open the case from that location.
  - During the case investigation, you might need to add a file, folder, drive, or image to a case. FTK uses the **Add Evidence** Wizard to add evidence to a case.
    - Open the case to which you want to add evidence. Click **File**, and then **Open**. Select the case.ftk file for the appropriate case
    - Click **File**, and then **Add Evidence**. The **Add Evidence** Wizard opens.
    - Enter the investigator's name.
    - Check the processes that you want run on the evidence.
    - Add the evidence.
    - Review your evidence selections.
    - Complete the wizard to launch the processing of evidence.

# Practical No: 02

**Title:** Exploring AccessData FTK

**Tools Used:** AccessData FTK

## Tasks to be performed:

- **Data Carving**
  - **Data Carving Files During Evidence Processing in a New Case**
    - Click on **Tool** Menu ➔ Select **Data Carving**
    - Check the file types to carve. (here we will select image files)
    - Click **OK**
  - **Data Carving Files During Evidence Processing in a Existing Case**
    - Click on **Tool** Menu ➔ Select **Data Carving**
    - Check the file types to carve. (here we will select image files)
    - Check the **Automatically Add Carved Items to Case** option. The**Minimum Image Size** fields activate. Specify a minimum size in pixels in which to display images. The program will question you about minimum sizes over 480 pixels.
    - Click **OK**
  - **Adding Carved Files to the Case**
    - Select the files you want to add to the case.
    - Click **Add Items to Case.**
    - Click**Yes**to accept the default name**.**Else click **No,** enter a different name, and click **OK.**
- **Filters**
  - **Applying an Existing Filter**
    - To apply an existing filter, use the Filter drop-down list on the **File List toolbar**
  - **Using The File Filter Manager**
    - Click on **View** Menu ➔ Select **File Filter Manager**
    - The following sections review the categories in the File Filter Manager menu:
      - **Legend**: The Legend identifies the individual filter settings that can be selected for each item. Click an item in the Legend to apply the setting to all items in the **File Status** and **File Type** columns.
      - **File Status**
      - **File Type**

- **File Size**
- **File Date**

# Practical No: 03

**Title:** Using File Recovery Tools

**Tools Used:** AccessData FTK Imager

**Tasks to be performed:**

- **Creating a new disk image of the drive (in our case we will create a image of the 4GB/2GB pen drive)**
  - **Create a raw image**
    - Start **FTK Imager**➔ Click on **File** Menu ➔ Select **Create Disk Imager**
    - **Select Source** dialog box will be displayed ➔ Select option **Physical Drive**➔Click **Next**
    - In **Select Source** dialog box, select the drive (pen drive) from the **dropdown** of which disk image needs to be created. And click **Finish**.
    - In the **Create Image** dialog box
      - **Select all the three checkboxes**:
        - Verify image after they are created
        - Precalculate Progress Statistics
        - Create directory listings of all the files in the image after they are created
      - Click on **Add** button ➔ Choose option **AFF** in the **Select Image Type** dialog ➔ click **Next**
      - In the **Evidence Information** Form, enter the following details:
        - In the **Case Number** field, enter the case number for reference.
        - In the **Evidence Number** field, enter the evidence number of the case
        - In **Unique Description** field, enter the evidence description for that case.
        - In **Examiner** field, enter the name of the examiner of this evidence.
        - In **Notes** field, any comment that is related to the evidence can be added
      - Select the locationwhere you want to store the image of the drive by clicking on **Browse** window in the **Select Image Destination** dialog box. ➔ to encrypt the image file select checkbox **Use AFF Encryption**➔ **AFF Encryption** dialog will appear.
      - Enter the **password** and **Re-enter** the password. Make sure both the password matches. Click **OK**.

- Click **Finish**.
- Click on **Start** button in the **Create Image** dialog box to start creating the image of the drive

- 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
- 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
- Click on **Image Summary** button to view the image summary.
- **Finding about the drive:**
  - **Drive Model Name:**
  - **Removable:** True/False
  - **Source Data Size:**
  - **Source Type:**
  - **Cylinders:**
  - **Tracks per Cylinder:**
  - **Sectors per track:**
  - **Bytes per Sector:**
  - **Sector Count:**
  - **MD5 Hash:** Matched /Not Matched
  - **SHA1 Hash:** Matched/Not Matched
  - **Bad Sector List:** Found / Not Found

# Practical No: 04

**Title:** Using Email Forensics

**Tools Used:** AccessData FTK

## Tasks to be performed:

- **Starting a new case**
  - Start the AccessData FTK. From **File** menu➔Select**New Case.**
    **or**
  - In case you are opening the FTK for the first time, **FTK Start up Screen** is displayed ➔ Select **Start a New Case** option ➔ Click **OK.**
  - **Enter basic case information.**
    - The New Case form provides fields for basic case information, such as the case name and its investigator.
      - In the **Investigator Name** field, type the name of the investigator.
      - In the **Case Number** field, enter the case number for references.
      - In the **Case Name** field, enter the name of the case.
      - Next to the **Case Path** field, click **Browse** to select the path where the evidence will be stored.
      - Verify that the **Case Folder** field lists the folder where you want the case to be stored.
      - In the **Case Description** field, add information that will be helpful to the analysis of the case.
      - Click on **Next**

  - **Entering Forensic Examiner Information**
    - The Forensic Examiner Information form allows you to enter information about the forensic examiner.
      - In the **Agency/Company** field, type the name of the agency or company.
      - In the **Examiner's Name** field, type the name of the examiner.
      - In the **Address** field, enter the address for the agency/company.
      - In the **Phone** field, enter the phone number for the agency/company.
      - In the **E-Mail** field, enter the examiner's e-mail address.
      - In the **Comments** field, enter any necessary comments.
      - Click on **Next**

  - **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.
- In the **Case Log Options form**,
  - Select what you want to include in the case log.
  - Click **Next**.

- **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.
  - In the **Evidence Processing Options form**:
    - Select the processes that you want to be run on the evidence.
    - Click **Next**.

- **Refining the Case**
  - Click on "**Include all Item**" in the Refine Case Form.
  - Select the **File Status criteria**.
  - Select the **File Type criteria**.
  - Click **Next**.

- **Refining the Index**
  - Select which items you want to unconditionally index.
  - From the drop-down list, indicate whether you want to index items that satisfy boththe File Status and File Type criteria and items that satisfy eitherthe File Status or File Type criteria.
  - Select the **File Status criteria**.
  - Select the **File Type criteria**.
  - Click **Next**.

- **Adding Evidence**
  - In **Add Evidence Form**, click on **Add Evidence** button.
  - Select **Individual File** option and click **Continue.**
  - Select **Jim_shu's.pst** from the Desktop and click **Open**.
  - In the **Evidence Information** Form, enter **Evidence Identification Name/ Number** and **comment** if required. Click **OK**.
  - Evidence will be added in the **Add Evidence Form**. Click **Next**.

- **Reviewing Case Summary**:

- In the Case Summary Form if you want to change or review any selections, click **Back** to return to the appropriate form. After you make your changes, click **Next** to return to the Case Summary form.
- To accept the current settings and start the processing of the evidence, click **Finish**.

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

## • View the Emails and perform Search

- **To view the email and its content:**
  - In the **Overview** tab of the **AccessData FTK**, Click on the **Email Messages** button under the **File Category** section.
  - Now open the **E-Mail tab**, and select **Unfiltered** option from the filter dropdown.
  - On the left hand side, in the **tree view** click on the folders.
  - To view the email in the **viewer** (lower pane), click on the messages in the **file list** (right hand side pane)

- **Create a bookmark on the e-mail messages:**
  - Select the checkboxes next to messages from the **file list** of the **E-mail** tab.
  - Select **Create Bookmark** from the **Tools** Menu.
  - Create **Bookmark** form is displayed. Enter the **Bookmark Name** & **Bookmark comment**.
  - Click on **All checked items**.
  - Select option **Include in Report** from the **Report Options** and check the checkbox next to **Include parent of email attachments**.
  - Click **OK**
  - Go to **Bookmark** tab, click on the name of the bookmark in the **tree view**, you will be seeing the messages that you have bookmarked.

- **To perform search in using list of words:**
  - Click on the **Search** tab. In Search tab, click on **Indexed Search** tab.
  - In the **Search Term** field, enter the term that you want to search e.g. “spec” and click on **Add**.
  - In the **Search Term** field, enter the one more term that you want to search e.g. “bike” and click on **Add**.
  - In the **Search Term** field, enter the one more term that you want to search e.g. “december” and click on **Add**.

- In **Search Item** pane, you will find the search result hits with **AND** combination. Click on **OR** button to view the changes in the hit in the search result.
- Click on **AND**. Click **View Cumulative Results** and select **All files** from the **Filter Search Hits and** Click **OK**.
- In **Search Result list**, the number of hits to the file will be displayed and also the messages that contain the search terms and their occurrence will be highlighted.
- When clicked on the hits in the search result list the message will be displayed in the **Viewer**.

- **Email Header fields and its description**

| Field Name | Description |
|---|---|
| From | E-mail address (sometimes names) of the author(s) of the e-mail |
| To | The e-mail address(es) (sometimes names) of the message recipient |
| Cc | Carbon Copy |
| Bcc | Blind Carbon Copy |
| Subject | A summary of the topic |
| Date | The local time and date when the message was written |
| Reply-to | Address that e-mail reply will redirected to |
| Message-ID | Globally unique message identification string generated when it is sent |
| References | Identifies other documents related to this message, such as other e-mail message |
| Received | Tracking information generated by mail servers that have previously handled a message, in reverse order |

# Practical No: 05

**Title:** Writing Report using FTK

**Tools Used:** AccessData FTK

## Tasks to be performed:

- **Opening the Existing case:**
  - Start the AccessData FTK. From **File** menu➔ Select **Open Case.**
    **Or**
    In case there is not existing case, create a new case (refer to practical no: 01) and proceed from the next step.
- **Create Bookmarks:**
  - **Create a bookmark on the e-mail messages:**
    - Click on **E-mail Messages** under the **File Category** section of the **Overview** Tab.
    - Click on **E-mail** tab.
    - Select **Create Bookmark** from the **Tools** Menu.
    - Create **Bookmark** form is displayed. Enter the **Bookmark Name** & **Bookmark comment**.
    - Click on **All the currently listed items**.
    - Select option **Include in Report** from the **Report Options** and check the checkbox next to **Include parent of email attachments**.
    - Click **OK**
    - To add messages to the bookmark, **select few messages** from the **file list** of the **E-mail tab**.
    - Select **Add to Bookmark** from **Tools** Menu.
    - In **Add File(s) to Bookmark**, select **All Checked items**. And click on the name of the bookmark in which you want to add the items.
    - Click **OK**
    - Go to **Bookmark** tab, click on the name of the bookmark in the **tree view**, you will be seeing the messages that you have bookmarked.

  - **Create a bookmark on the documents:**
    - Click on **Documents** under the **File Category** section of the **Overview** Tab.
    - Highlight few of the documents from the **file list**.
    - Select **Create Bookmark** from the **Tools** Menu.
    - Create **Bookmark** form is displayed. Enter the **Bookmark Name** & **Bookmark comment**.

- Click on **All highlighted items**.
- Select option **Include in Report** from the **Report Options** and check the checkbox next to **Include parent of email attachments**.
- Click **OK**
- To add messages to the bookmark, **select documents** from the **file list** of the **Overview**tab.
- Select **Add to Bookmark** from **Tools** Menu.
- In **Add File(s) to Bookmark**, select **All Checked items**. And click on the name of the bookmark in which you want to add the items.
- Click **OK**
- Go to **Bookmark** tab, click on the name of the bookmark in the **tree view**, you will be seeing the messages that you have bookmarked.

- **Create a bookmark on the graphics:**
  - Click on **Graphics** under the **File Category** section of the **Overview** Tab.
  - Highlight few of the messages from the **file list** of the **Graphics** tab.
  - Select **Create Bookmark** from the **Tools** Menu.
  - Create **Bookmark** form is displayed. Enter the **Bookmark Name** & **Bookmark comment**.
  - Click on **All highlighted items**.
  - Select option **Include in Report** from the **Report Options** and check the checkbox next to **Include parent of email attachments**.
  - Click **OK**
  - To add messages to the bookmark, **select documents** from the **file list** of the **Graphics** tab.
  - Select **Add to Bookmark** from **Tools** Menu.
  - In **Add File(s) to Bookmark**, select **All Checked items**. And click on the name of the bookmark in which you want to add the items.
  - Click **OK**
  - Go to **Bookmark** tab, click on the name of the bookmark in the **tree view**, you will be seeing the messages that you have bookmarked.

## • Creating a Report

- Click on **File** menu and select **Report Wizard**.
- **Entering Basic Case Information**
  - If you want to include the investigator information, check the **Include Investigator Information in Report** box. Else click **Next**.
  - The following details needs to be filled if you want to include the investigator information to be included in the report:

- In the **Agency/Company** field, enter the name of the organization that analyzed the case.
- In the **Investigator Name** field, type the name of the investigator.
- In the **Address** field, enter the investigator's address.
- In the **Phone** field, enter the investigator's phone number.
- In the **Fax** field, enter the investigator's fax number.
- In the **E-mail** Address field, enter the investigator's e-mail address.
- In the **Comments** field, enter the comments pertinent to the report.
- Click **Next**.

- **Managing Bookmarks**
  - **Bookmarks-A**
    - The Bookmarks-A form allows you to create a section in the report that lists the bookmarks that were created during the case investigation.
    - **Choose the appropriate option/s** under each section of Bookmark-A form.
    - Click **Next**.

- **Selecting the Properties of Bookmarked Files**
  - **Bookmarks-B**
    - The Bookmarks-B form allows you to select which file properties to include for each bookmarked file.
    - If you chose to not include a bookmark section, this form does not appear in the wizard.
    - If you want to modify the file property list, click **Add/Remove File Properties**.
      - In the Load from Stored Column Settingsdrop-down list, select the template that contains the file information that you want to include in the Bookmark section of the report.
        - If you want to **define a new column** settings template:
          - **Check or uncheck the Column Names**, depending on which ones you want to include in the setting. You can click **Select All** or **Unselect All** to mark or unmark all the columns.
          - To change the order in which the columns appear in the **File List**, select a column name and click **Move Up** or **Move Down**.
          - To create a new column setting, click **Save As**, enter a name in the field, and click **OK**.

- If you want to **modify an existing template**:
  - Click **Columns**.
  - Select the **column setting** you want to modify.
  - Modify the **Column Settings** form.
  - Click Save, then**Close**, and then**OK**.
- Click **Next**.

- **Managing Thumbnails**:
  - The Graphic Thumbnails form allows you to create a section in the report that displays thumbnail images of the case graphics.
  - **Choose the appropriate option/s** under each section of **Graphic Thumbnail** form.
  - Click **Next**

- **Selecting a File Path List**
  - The **List by File Path** form allows you to create a section in the report that lists the file paths of files in selected categories. The List by File Path section simply displays the files and their file paths
  - In the **List by File Path** form
    - Check the **Include in the Report** box. The **Include column** of the selected categories changes to "**YES**."
    - If you want to export and link to the files in the File Path list, check the **Export to the Report**box.
    - If you want to use a filter to manage which files appear in the **File Path list**, check the **Apply a File Filter** to the List box and select the filter from the Filter Namedrop-down list.
    - Click **Next**.

- **Selecting a File Properties List**
  - The List File Properties-A form allows you to create a section in the report that lists file properties for files in selected categories.
  - In the **List File Properties** form:
    - If you want to include the list, check the **Include a List File Properties Sectioninthe Report**box.\
    - If you want to include an MS Access database, check the **Include MS Access database in Report**box.
    - In the Categories of Lists to Be Included in the Report list, select which file categories to include in the list.
      - Check the **Include in the Report** box. The **Include column** of the selected categories changes to "**YES**."

- If you want to export and link to the files in the File Path list, check the **Export to the Report** box.
- If you want to use a filter to manage which files appear in the **File Path list**, check the **Apply a File Filter** to the List box and select the filter from the Filter Name drop-down list.

- Click **Next**.

- **Selecting the Properties of the File Properties List**
  - The **List File Properties-B** form allows you to select which file properties are displayed for files in the categories specified in the previous form. This form only appears if you chose to create the List File Properties section in the report.
  - **Choose the appropriate option/s**under each section of **List File Properties-B** form.
  - Click **Next**.

- **Adding Supplementary Files and the Case Log**
  - The Supplementary Files form allows you to add files such as hash lists or search results to the report.
  - In the **Supplementary Files** form:
    - If you want to add supplementary file, click **Add Files** and browse to the file you want to include in the report.
    - If you want to remove a file, select the file in the Supplementary Files window and click **Remove File**.
    - If you want to add the case log to the report, check the **Include Case Log in Report** box.
    - If you have created an HTML file list in preprocessing, you can add it to your reports by checking the checkbox next to **Include HTML file list in preprocessing**.
    - Click **Next**.

- **Selecting the Report Location**
  - The Report Location form allows you to select the location of the report. You can also add a customized graphic, such as the logo of your organization, and include Registry Viewer reports.
  - In the **Report Location** form:
    - In the **Report Folder** field, browse to and select the location for the report folder.
    - If you have created registry reports in Registry Viewer or FTK, check the **Include Registry Viewer Reports** box to include those reports in

your FTK case report. This includes any Registry Summary Reports (RSRs) you have created and selected in FTK.

- If you want to include a custom graphic in the report, check the **Custom Graphic for the Report** box. Click **Browse**to select the graphic from the directory tree.
- Select the language for the report from the **Report Language** drop-down list.
- Click **Finish**.

- **Viewing a Report**
  - **To view the report in FTK:**
    - Immediately after creating the report, click **Yes** to view the report.
    - Select **File**, and then **View Report**. Browse to and select the **\case_name\report\ directory**.

# Practical No: 06

**Title:** Using Steganography Tools

**Tools Used:** S-Tools

## Tasks to be performed:

- **Encrypting and decrypting text file into/from image file (bmp/gif).**
  - **Encrypting text file into image file**
    - Open **S-tools**
    - Simply drag the image file (zebra.bmp) over an empty space in the **S-Tools Window**.
    - **Create a text file** named input.txt and add some text into the file.
    - Drag the text file (input.txt) over the image window in the S-Tools.
    - **Security dialog box** is displayed by the S-tool. Enter the **Passphrase** and **Verify Passphrase**. Make sure that you have entered same value for Passphrase and Verify Passphrase. Remember the passphrase.
    - **Choose one algorithm**from the dropdown in the security dialog box for encryption of the file and click **OK**.
    - New window will open in the S-tools with named **hidden data**. **Right click on the hidden data** window. Choose option **Save as** and save the file with the same extension as the input image file(hid_zebra.bmp)

  - **Decrypting text file from image file**
    - Right click on **hid_zebra.bmp** window and select **Reveal**.
    - **Security Dialog Box** will be displayed. Enter the **Passphrase** and **Verify Passphrase** that you had entered at the time of encryption. **Select the algorithm** from the dropdown that was used at the time of encryption.
    - **Revealed Archive** window pop-ups with the name of the file(input.txt) that you had encrypted in the image file.
    - Click on the file name (input.txt) in the **Revealed Window** and Right click. Select option **Save as** and save the file.

**Findings**

| Size of the image file before encryption | Size of the created text file | Size of the image file after encryption | Size of the text file received after encryption | Algorithm used |
|---|---|---|---|---|
| | | | | |

- **Encrypting and decrypting text file into/from sound file (wav).**
  - **Encrypting sound file into image file**
    - Open **S-tools**
    - Simply drag the sound file (ringout.wav) over an empty space in the S-Tools Window.
    - **Create a text file** named input.txt and **add some text** into the file.
    - Drag the text file (input.txt) over the sound window in the S-Tools.
    - **Security dialog box** is displayed by the S-tool. Enter the **Passphrase** and **Verify Passphrase**. Make sure that you have entered same value for Passphrase and Verify Passphrase. Remember the passphrase.
    - **Choose one algorithm** from the dropdown in the security dialog box for encryption of the file and click **OK**.
    - New window will open in the S-tools with named **hidden data**. **Right click on the hidden data window**. Choose option **Save as** and save the file with the same extension as the input sound file(hid_ringout.wav)

  - **Decrypting text file from image file**
    - Right click on **hid_ringout.wav** window and select **Reveal**.
    - **Security Dialog Box** will be displayed. Enter the **Passphrase** and **Verify Passphrase** that you had entered at the time of encryption. **Select the algorithm** from the dropdown that was used at the time of encryption.
    - **Revealed Archive** window pop-ups with the name of the file(input.txt) that you had encrypted in the sound file.
    - Click on the file name (input.txt) in the **Revealed Window** and Right click. Select option **Save as** and save the file.

**Findings**

| **Size of the sound file before encryption** | **Size of the created text file** | **Size of the sound file after encryption** | **Size of the text file received after encryption** | **Algorithm used** |
|---|---|---|---|---|
| | | | | |

# Practical No: 07

**Title:** File System Analysis

**Tools Used:**Autopsy

## Tasks to be performed:

- **Create a new case**
  - **Two ways to create a new case:**
    - The opening **splash screen** has a button to **Create new case**. Click on the button **Create new case**.
    - Click on **File** menu and select **New Case**.
  - **New case Wizard:**
    - New case wizard will be displayed on the screen.
    - Enter the following information in the **Case Info** section of the **New case wizard**:
      - In **Case Name** field, enter the case name.
      - For entering the path in the **Base Directory**, click on the **Browse** button and browse to the folder where you want to save the case. A directory for the case will be created inside of the "base directory"
    - Enter the following information in the **Additional information** section of the **New Case wizard**:
      - In **Case Number** field, enter the case number. This field is optional.
      - In **Examiner** field, enter the examiner name. This field is also optional.
    - Click on **Finish**.

- **Adding Source to the case:**
  - Autopsy supports **three types** of data sources:
    - **Disk Image:** A file (or set of files) that is a byte-for-byte copy of a hard drive or media card.
    - **Local Drive:** Local storage device (local drive, USB-attached drive, etc.).
    - **Logical Files:** Local files or folders.
  - In this practical we will be adding a image file for analysis.
  - **Add Data Source Wizard:**
    - Fill the following details in **Enter Data Source Information** Section:
      - Select **Image File** option from the **Select source type to add** dropdown.
      - Click on **Browse** button to browse to **precious.img** file on the desktop and click **Open**.

- Click **Next**.

- While it is examining the data source, you will be prompted with a list of **Ingest modules** to enable.Click **Next**.
- After you configure the ingest modules, you may need to wait for Autopsy to finish its basic examination of the data source.
- Click On **Finish**.

## • Running the Ingest Module:

- **Run Ingest Module:**
  - Click on **Tools** menu, select **Run Ingest Module** and select the file.
  - **Ingest Module wizard** will be displayed.
  - Click on **Start** button. It will take some time to analyze the files.

## • Exploring precious.img in Autopsy:

- **Image details:**
  - Expand **Data Source** in the left pane, highlight **precious.img** and **right click** and select **Image Details**.

- **Search File by Attribute:**
  - Click **Tools** menu, select **File Search by Attribute**.
  - **File search by attribute** window will be opened. In this you can search file by **Name, Size, Date** and **Known status**.
  - Click on any (one or more) checkbox adjacent to the **Name, Size, Date** and **Known Status**. Fill the appropriate information and Click **Search** button.

- **Keyword Search Bar:**
  - Click on the **Keyword Search** in the toolbar.
  - Enter the keyword that you want to search in the text field adjacent to the Search button.
  - Select any one **radio button** out of **Exact Match, Substring Match, Regular Expression**.
  - Click on **Search** button.
  - Files which contain the keyword or the files which has the keyword as name of the file will be enlisted in the right pane.
  - Click on any file, you will see the keyword being highlighted in the file in the **indexed text** tab below.

- **Searching Using in-built keywords:**
  - Click on **Keyword List** in the toolbar.

- Click on **Manage List** button.
- Click on **New List**. Enter the keyword list name in the field of New keyword list name and click **OK**.
- Type the keyword (frodo, specs, December, bike) in the text field adjacent to **Add** button. If the keyword is the regular expression then check the checkbox adjacent to the Regular Expression. Click Add.
- After successfully adding the list of keywords, click **OK**.
- Check **Phone Number, IP Addresses, Email Addresses** & **URLs**. Also check the name of newly created list.
- Click on **Search**. The information will appear in the **Keyword Hits** section under the **Results** subtree.

- **Saving File Location:**
  - Right-click on the file you want to tag, point to **Tag File** and click **Quick Tags** and **New Tag**.
  - Enter the tag name in the **Tag Name** field and Click **OK**.
  - To see the list of files you have marked, expand **Tags** section in the left pane.

- **Viewing File types:**
  - Expand **Views** in the left pane. In view expand **FileTypes**.
  - In **FileTypes**, you will find all the different types of file of precious.img

- **Creating Bookmark:**
  - Click on **Images** under **File Types**.
  - Select **highlight few images** in **File List**, Right Click select **Tag Files**, click **Quick Tag** and then select **Bookmark**.
  - Similarly you can create a bookmark on other file types.
  - To see the list of filed you have bookmarked, expand **Tags** section in the left pane.

## • Creating a timeline:

- Click on **Tools** menu and select **Timeline**.
- **Autopsy timeline window** appears.
- To show the months when file activity took place, click the bar for the year you want to view. The graph updates to show the file activity for each month of the year.
- To show the days when file activity took place, click the bar for the month you want to view. The graph updates to show the file activity for each day of the month.
- To see the file activity for a particular day, click the day you want to view.

## • Generating a report

- **Creating a report:**

- Click on **Generate Report** in the toolbar
  or
  Click **Tools** menu and select **Generate Report**.
- Select option **Results-HTML** and click **Next**.
- Select **All Results** and Click **Finish**.
- Click **Close**.

- **View a report:**
  - To view the report **click on the link** given on the **Report Generation Progress wizard** after completion of report generation.

# Practical No: 08

**Title:** Using Data acquisition tools

**Tools Used:** ProDiscover Basic

**Tasks to be performed:**

- **Create a new project & saving project:**
  - **Create a new project:**
    - Start ProDiscover Basic.
    - ProDiscover Basic presents a **Launch Dialog**.
    - Enter the following details in the Launch Dialog:
      - In the **Project Number** field, enter the project number.
      - In the **Project Name** field, enter the name of the project.
      - In the **Description** field, enter the description of the project.
      - Click on the **Open** button.
      - ProDiscover Basic will then create a project & generate a template report in the work area.
  - **Save a project:**
    - Select **save** project option from the **file** menu, or button bar.
    - 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.
    - Select the destination path and click **Save** button

- **Adding image file to the project:**
  - Expand **Add** in the left pane.
  - Click on the **Image File** in the **Add** subtree. **Open** dialog will appear.
  - In the **Files of type** dropdown select **All Files (*.*)**.
  - Browse to the **Desktop** and select **precious.img** file.
  - Click **Open**.

- **View the content of the image file:**
  - Expand **Content View** in the left pane.
  - Expand **Images** under the **Content view**.
  - In the Images subtree you will find the path of precious.img.
  - When you **expand the path**, you will find the different directory of that image file.
  - Click on any directory, the list of files/folders will be displayed on the top right pane.

- **View Graphic Files in Gallery View:**
  - Click on **View** menu and select **Gallery View** option

- **Recovering a deleted file:**
  - Expand **Content View** and **Images** in the **Content View**.
  - **Expand the path** of the image file and in the directory, you will find **Deleted Files**.
  - Click on **Deleted Files**. The files that have been deleted from the drive will be shown in the top right pane
  - **Click on any the file** that you want to recover. **Right click** and select the option **Copy File**
  - **Save As** dialog box will be opened. Save the file with appropriate name and click **Save** button.
  - Now navigate to the folder on your system where you have saved the file. Open the file to see the content of the file

- **Search for keyword in the file:**
  - Click on **Search** in button bar. **Search** dialog will appear.
  - Select the appropriate options in the Search dialog. For example, we shall search for string ffd8ffe0 (jpeg header). In the **Content Search** tab of **Search** dialog, select **Hex** & **Search for pattern(s)** radio button. In the text field enter **ffd8ffe0**. In the **Select the Disk(s)/Image(s) you want to search in** select the path of the image file. And click **OK**.
  - You can find the searched information in **Content Search Results** under the **Search Result** in the left pane.

- **To view the Internet History and search for keyword in the internet history:**
  - **<u>To view the Internet History:</u>**
    - Expand **Content View** and **Images** in the **Content View**.
    - **Expand the path** of the image file and look for **Documents and Settings**.
    - Expand **Documents & Settings**. Highlight Frodo Baggins folder and right click.
    - Click on the option of **Find Internet Activity**.
    - To view the internet activity, expand the **Internet History Viewer** in the left pane.
  - **<u>Search for keyword in the Internet history.</u>**
    - Click on **Search** in button bar. **Search** dialog will appear**.**
    - Click on the **Internet Search History** tab.

- In the **Select the Internet Activity File you want to search in** dropdown select the files.
- In the **Look in** frame few options will be active. Select the appropriate option. For example select **URL, File Name, HTTP Header, Host Name**.
- Select the radio button next **ASCII**.
- In the **Search for the pattern(s)** text field enter rings, bike.
- Click **OK**.

- **Capture Image for Physical Memory:**
  - In the left pane, expand **Add**.
  - Click on **Capture and Add Image**. **Capture image** dialog will appear.
  - In the **Source Drive** dropdown select option **Physical Memory**.
  - Click on the **>>** button and select option **Choose Local Path**. **Save As** dialog will appear. Give the name of file, ex. Memanalysis and click **Save**.
  - Click **Split** button. **Split Image** dialog will appear. In **Split into equal sized image of** text box enter **1024**. And click **Split** button. Click **Update** and then click **OK**.
  - Enter **Technician Name** and **Image number** in the text boxes.
  - Click **OK**.

- **Generate report:**
  - Click on the **View** menu and select **Report**.

# Practical No: 09 & 10

**Title:** Using log capturing and analysis tools&Using traffic capturing and analysis tools

**Tools Used:**Wireshark

**Tasks to be performed:**

- **Create a new windows account**

**Start**

# Practical No: 11

**Title:** Using Password Cracking Tools

**Tools Used:**Cain and Abel

**Tasks to be performed:**

- **Create a new users account**
  - **Start ➔ Setting ➔ Control Panel ➔ User Accounts ➔ Create a new account**
  - Enter the name of user account in the text field (Ex. udit1) and click **Next**.
  - Select **Computer Administrative** radio button and click on **Create Account**.
  - On User Account window, you can see the name of the account that you had created.
  - Click on the name of the account.
  - Click on **Create a password**.
  - Type **password**and **retype the password** in the text fields, also enter the **phrase** and click on **Create password**.

- **Cracking password using Cain and Abel:**
  - Start **Cain and Abel tool** and click on **Cracker** tab.
  - Highlight **LM & NTLM Hashes** in the left pane and click on the + sign on the toolbar.
  - In **Add NT Hashes Form**, select **Import Hashes from local system** and click **Next**.
  - **Select a user account** (udit1) from the username and right click. Select **Dictionary Attack** and then click **NTLM Hashes**.
  - In the **Dictionary Attack form**, right click on the **Dictionary** section and select **Add to list**.
  - In browse to the **wordlist folder** and select **Wordlist.txt** and click **Open**.
  - Click **Start**.
  - If the tool is able to crack the password, the password will be displayed in the text section of the Dictionary Attack form.
  - The password will also be displayed in the **Cracker** tab for that username.

- **Sniffing & ARP Poisoning:**
  - Click on the **Sniffer** tab in the **Cain & Abel** tool.
  - In the **toolbar**, click on the **start/stop sniffer** icon next to the folder icon.
  - Select on the device in the **Configuration Dialog** and click **OK**.
  - **Click on the + button** in the **toolbar**. Select **All hosts in my subnet** in the **MAC Address Scanner** dialog and click **OK**.
  - The list of the connected host will be enlisted in the **Hosts** tab of **Sniffer** tab.

- Click on the **APR** tab of the **Sniffer** tab. The **Configuration/Routed Packets** will be displayed.
- Click on the + button in the toolbar. **Select an IP address** in the **New ARP Poisoning Routing** dialog box. Click **OK**.
- Now click on **Start/Stop ARP** icon in the **toolbar**.
- On the source IP Address, open any website like facebook, gmail or yahoo.
- Enter username and password in the website.
- Click on the **Password** tab of the **Sniffer** tab in the Cain and Abel tool.

# Practical No: 12

**Title:** Using Mobile Forensic Tools

**Tools Used:** Mobiledit

**Tasks to be performed:**

- **Install Mobiledit:**
  - Ensure that you install all phone drivers (Android)
  - When connecting the phone to the computer, it will ask for installing a connector apk in the phone. Install that apk in the phone.
- **Ensure that developers option and USB debugging is enabled in your mobile phone.**
- **Connect the mobile phone and Mobiledit tool:**
  - Start MOBILedit Forensic tool. **MOBILedit Connection Wizard** will be displayed.
  - Choose **Android** Radio button and click **Next**.
  - In Connection Type Select **Cable** radio button and click **Next**.
  - Connect the mobile phone using USB cable to the computer
- **Enable Developer option and USB debugging:**
  - **Enable Developer Mode:**
  - **Enable USB Debugging:**
  - Once the phone is listed, click **Finish**.
  - Click on the mobile device image shown on the screen and it will ask for installation of apk on the mobile device. Click **Yes**. It will install the apk on the mobile device.
- **View the data of the Mobile Device:**
  - Click on the Mobile Device icon in **MOBILedit**tool**.**
  - On the left hand there is navigation pane. In navigation pane, click on the **Connected**.
  - You will find your mobile device name in the subtree of connected.
  - **View Phonebook:**
    - Click on the **PhoneBook** in the left pane. All the contacts of the mobile device will be displayed on the screen.
  - **View Call Logs:**
    - Click on the **Call Logs** in the left pane. All the call logs of the mobile device will be displayed on the screen.
  - **To view the Image files:**
    - Select any image and click on **Photo Viewer** in the left pane. The image will be displayed.
  - **To view Hex Dump of the file:**

- Click on Hex Dump in the left pane. Next to left pane mobile device directory tree will be displayed.
- Navigate to the folder whose Hex dump to want to view. Click on the file and the Hex Dump of the file will displayed.

- **Generate Report:**
  - Click on **Forensic Report** in the **Navigation Pane** on the left. It will ask the format on which the report needs to be generated. Choose **XML**. **MOBILedit Forensic Report** window will be displayed. In **Device Capabilities**, select the checkboxes next to the features of mobile device and click **OK**.
  - **Report will be generated and displayed in the browser.**