Creating a Case

One of the most powerful features of EnCase® software (EnCase) is its ability to organize different types of media together so that they can be searched as a unit rather than individually. This process saves time and allows the examiner to concentrate on examining the evidence.

Case Management

Before starting an investigation and acquiring media, consider how to access the case once it has been created. It may be necessary for more than one investigator/examiner to view the information simultaneously. In such a case the evidence files should be placed on a central file server and copies of the case file should be placed on each examiner's computer (since case files cannot be accessed by more than one person at a time).

The EnCase® Forensic methodology strongly recommends that you use a second hard drive or at least a second partition on the boot hard drive for the acquisition and examination of digital evidence. It is preferable to wipe an entire hard drive or partition rather than individual folders to ensure all of the previous examination-related data is destroyed. This will aid in deflecting any claims of comingling of data from other examinations if the hard drive is used in other cases. The volume should also contain a unique volume label as well as a unique directory structure for proper case management.

One method of organization is to create a folder for each case and to place the associated case file and files supporting the examination efforts in that folder. Reports and evidence copies can then be placed in the same folder or in subfolders. Files representing the acquisition of digital evidence may be placed on a second hard drive or elsewhere as discussed previously.

EnCase automatically creates several folders when the case is created.

These folders include: Documents, Email, Export, Searches, Tags, and Temp. When a device or evidence file is added to the case, the EvidenceCache folder is created.

Create the Cases folder on the designated drive.

The EvidenceCache folder will be used to contain output from Processing and Device cache operations. The Export folder provides a general destination folder for data copied from the evidence file. The Tags folder documents items that the user has marked by category. The Temp folder allows the segregation and control of the temporary files that are created in the course of the investigation (discussed later). The Email folder is discussed within other GSI Training courses.

Start EnCase and click on the **New Case** link.

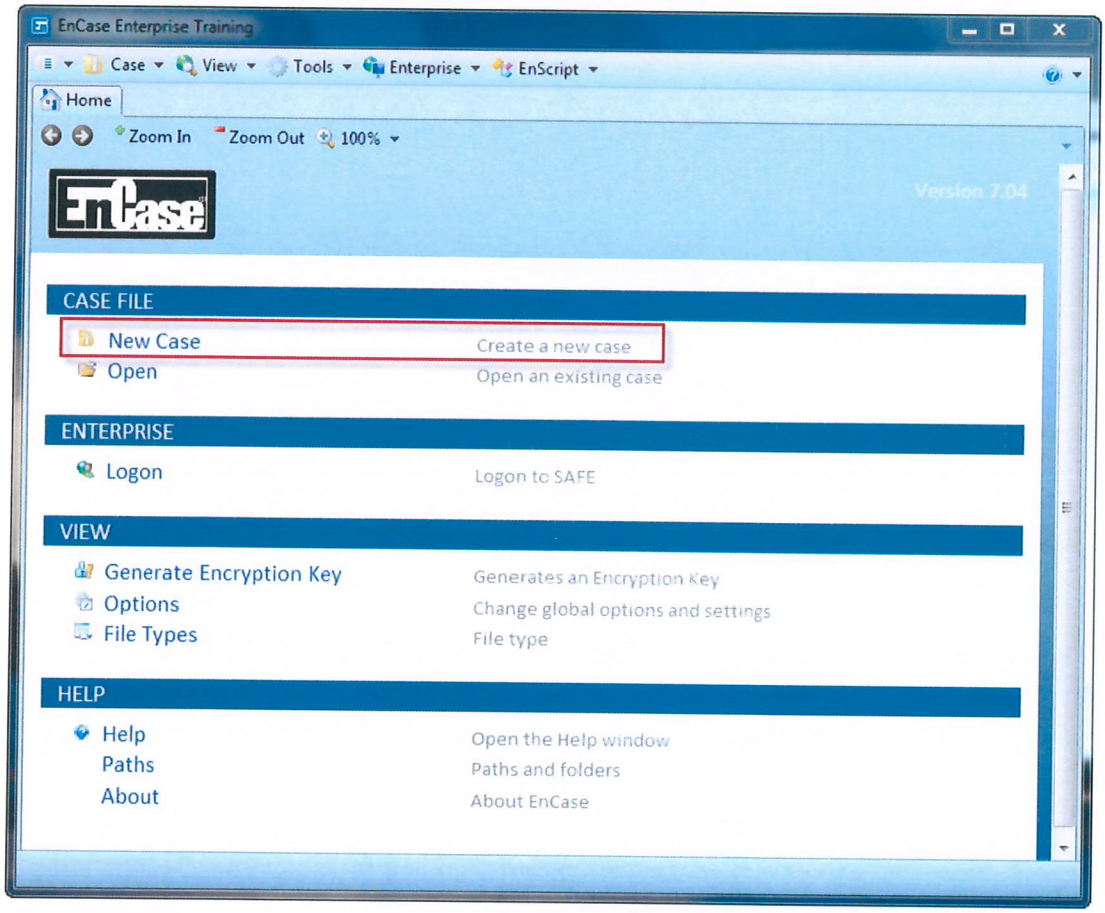

Figure 1-1 Click "New Case" option

The Case Options dialog box will appear. We will create a new case called "LocalSystem" with the base case folder defined within \Cases on the designated drive. The base case folder will be used for the primary evidence cache. The Basic (default) template should be used.

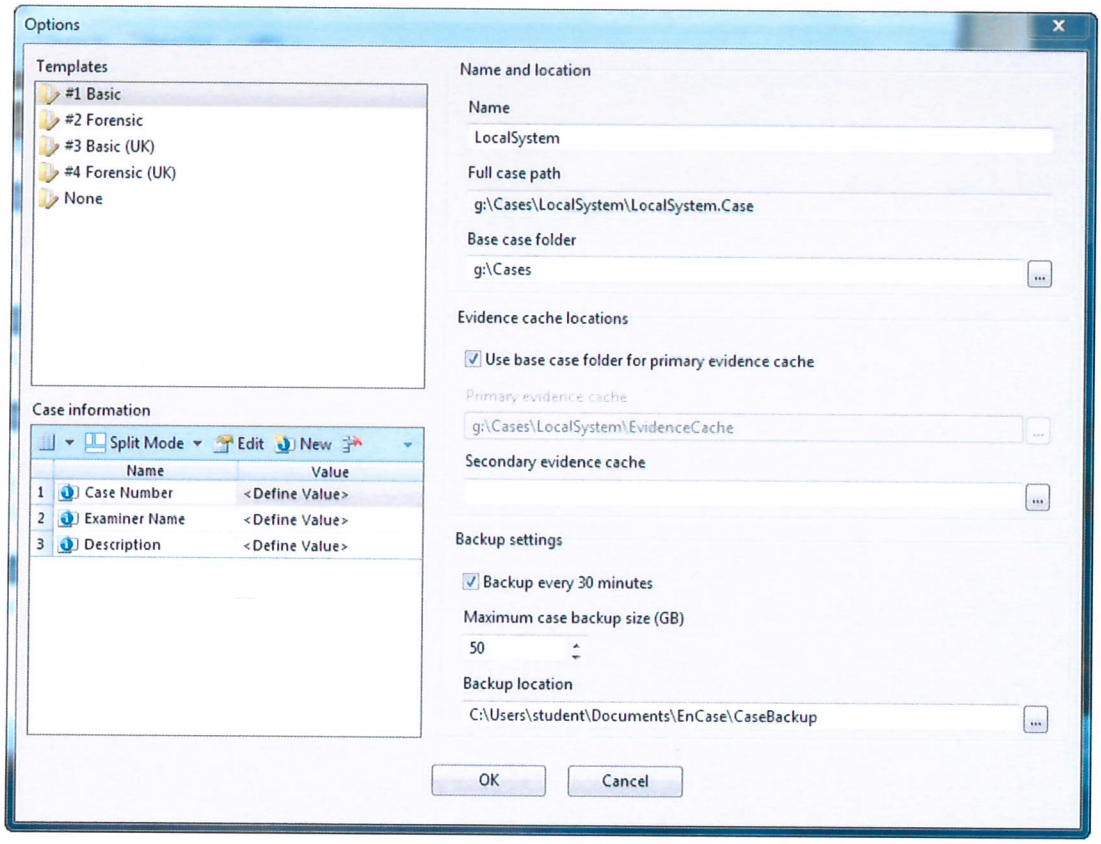

Figure 1-2 Case Options

1. **Templates** allow selection of a template containing preconfigured data for a case. Two fundamental templates are provided with EnCase: Basic and Forensic, which will be discussed later. EnCase provides templates with the default installation, however, any case structure may be saved by the examiner as a template to be used later. This configuration may consist of:
   - Case info items with default values (administrative information)
   - Bookmark folders and notes (to organize data for reporting)
   - Tag names (to mark important or irrelevant objects)
   - Report templates
   - User-defined report styles

2. The (case) **Name** is the file name representing the case stored on media.
3. The **Base case folder** is the default location where the case file will be saved. The initial default is the My Documents folder of the user.
4. The **Full case path** is the combination of the base case folder and the case name.
5. **Primary evidence cache** folder will contain, among other things, the results of the evidence processing operation. The default folder name is "EvidenceCache," and is stored by default within the My Documents folder of the user. EnCase uses cache files to speed up application responsiveness, enhance stability, and provide scalability across large data sets. The evidence processing may be performed and the results may be made available to multiple examiners in a centralized location. Although there is an evidence cache for each device in a case, it does not need to be stored in the same location as the evidence file. The EvidenceCache folder is not created until previewed drives or evidence files are linked to the case. Data will be stored within this folder when the Evidence Processor is run.
6. The option **Use Base Case Folder for Primary Evidence Cache** has been selected to put data for a case within the case folder structure.
7. The **Secondary evidence cache** folder designates an additional path where previously created evidence cache may be found. This allows users to specify on a network share or other location where cache files may be stored. Unlike the primary evidence cache folder, EnCase will only read previously created files from this location. All new files will be stored in the Primary evidence cache folder.
8. The **Case information** items are user-configurable, name-value pairs that document administrative information about the current case. These items are primarily used to insert user-definable information into a report template. The basic template includes three defined fields; more may be added. The forensic template includes additional fields. In this course, we will use the basic template.

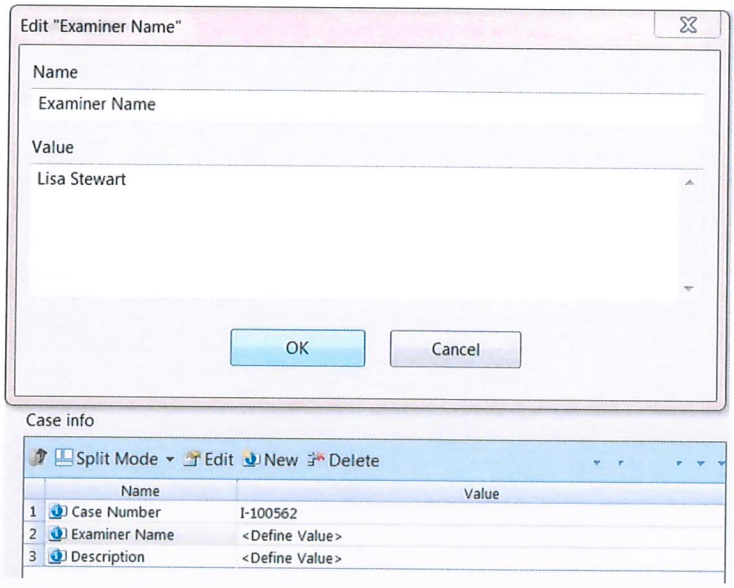

Figure 1-3 Case Info Values from basic template

9. The Backup Settings section has been added with EnCase 7.04. The backup defaults to every 30 minutes and has a backup maximum threshold. There may also be a backup location designated – the default backup location is within the Users folder structure. For our purposes, the default location will suffice.

Enter the appropriate information; click **OK**. The Home page for the case now appears.

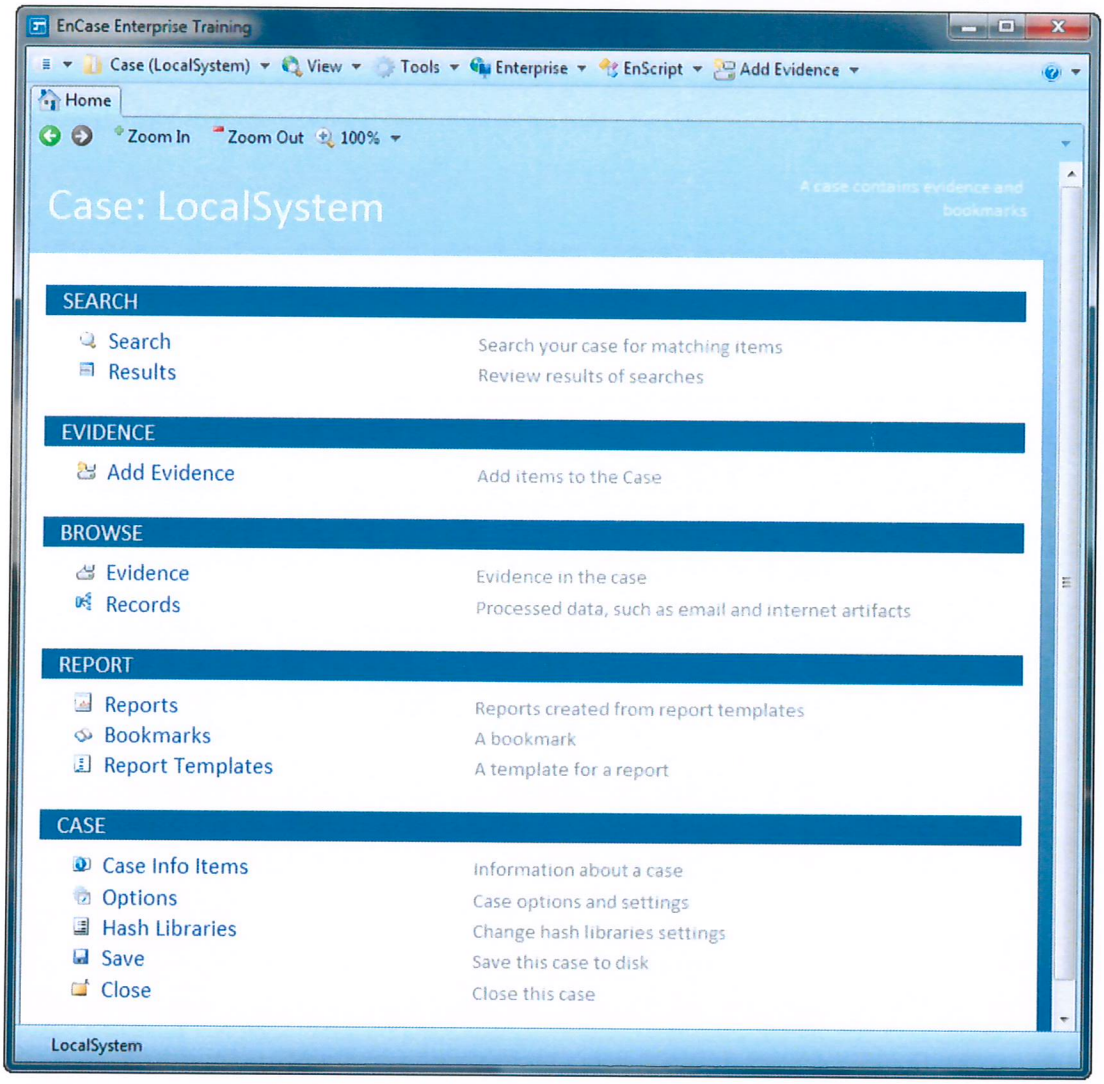

Figure 1-4 Case Home page

The case should automatically be saved in the E:\Cases\LocalSystem folder. To save the case manually, click the pull-down menu on **Case (LocalSystem)** and click on **Save**.

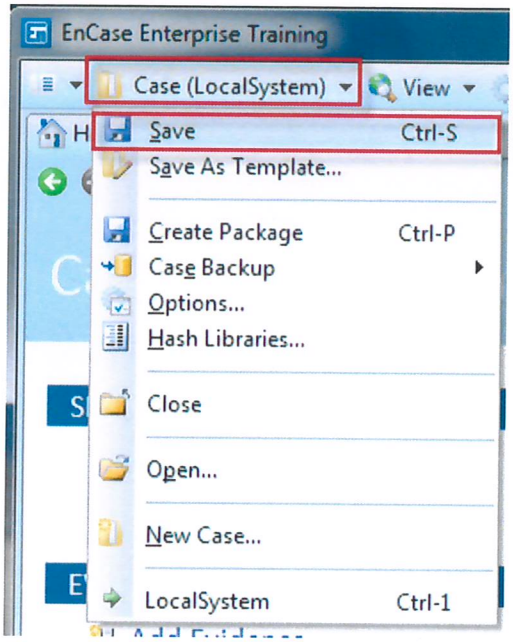

Figure 1-5 Case –Save case

To recall case settings, click on **Case→Options**. The options for the current case will appear.

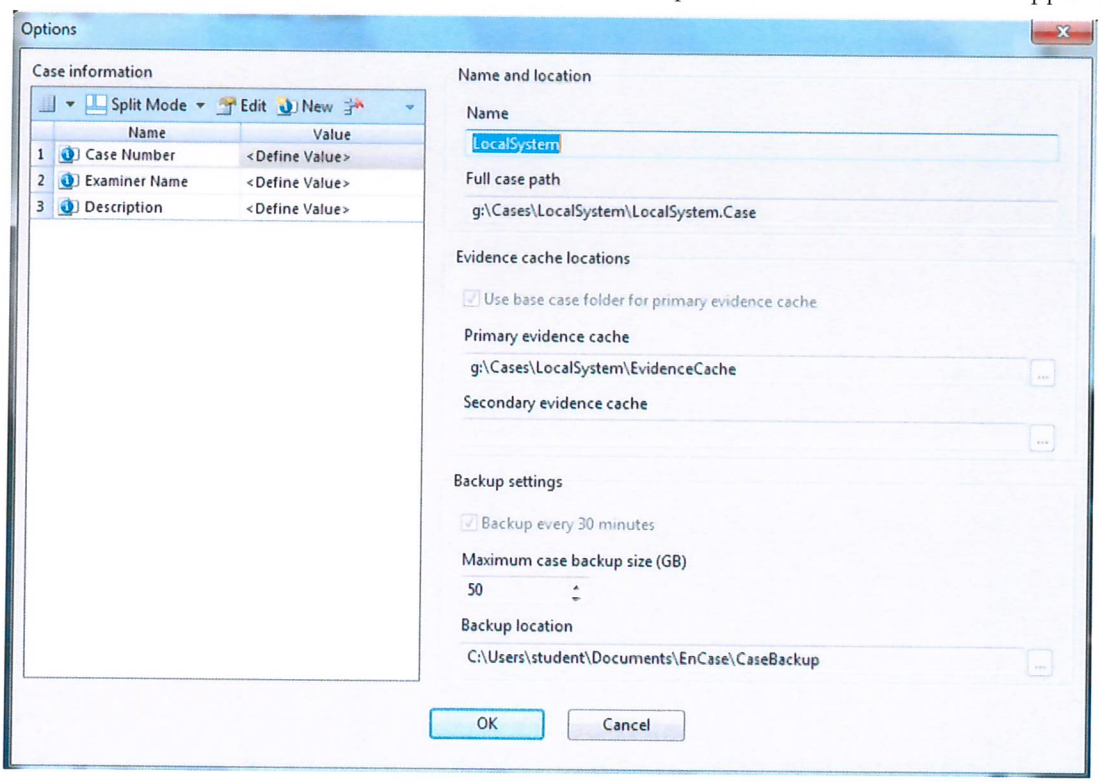

Figure 1-6 Case administrative options

EnCase configuration settings, which are global, may be found by selecting **Tools→Options**.

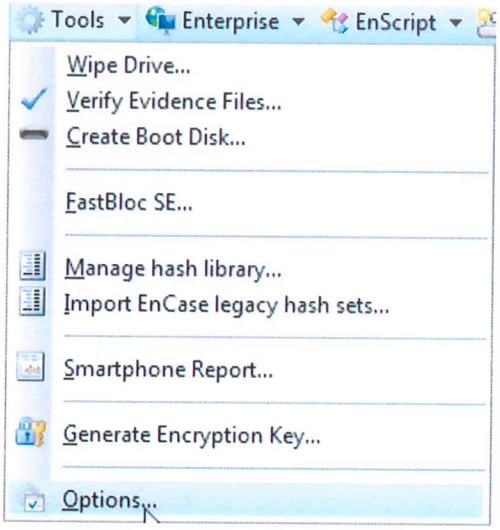

Figure 1-7 Access Options menu to configure EnCase

The **Global** tab allows various features to be changed, including the Code Page, picture, and timeout options.

The **Date** tab provides date/time format options.

The **NAS** tab contains all of the settings needed to enable the network authentication of the EnCase dongle if on a server.

The **Colors** tab provides the ability to set the color scheme for different elements of the EnCase® interface.

The **Fonts** tab can alter screen fonts; typically used for foreign language support.

The **Shared Files** tab designates the shared files folder, which provides easy access to shared EnScript® modules, filters, conditions, and keywords. These items, which provide valuable functionality to EnCase, will be discussed later.

The **Debug** tab is utilized by EnCase users who experience abnormal shutdowns or program lockups and by those working with customer service to determine the nature of the problem.