Lesson 1

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 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 investigator's computer (since case files cannot be accessed by more than one person at a time).

One method of organization is to create a folder for each case and to place the associated case file and evidence files in that folder. Reports and evidence copies can then be placed in the same folder or in subfolders. Creating a **Temp** folder in that folder allows the segregation and control of the temporary files that are created in the course of the investigation. The **Export** folder provides a general destination folder to place data copied from the evidence file (discussed later). The **Index** folder will be used and explained in a later lesson. An **Evidence** folder will be used to hold all forensic images of devices we acquire during our examination.

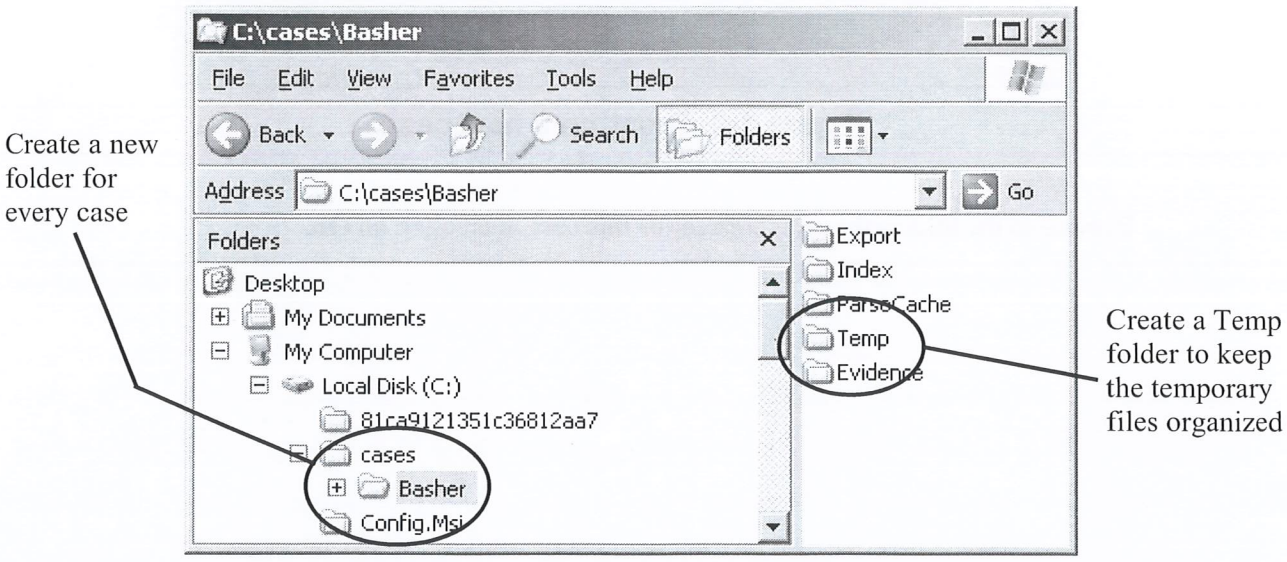

Figure 1-1 Creating folder structure

The EnCase® Forensic methodology strongly recommends that the examiner 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 temporary, suspect-related data is destroyed. This will aid in deflecting any claims of cross-contamination by the opposing counsel if the forensic hard drive is used in other cases.

Start EnCase and select **File→New** or click on the **New** icon on the toolbar. The Case Options dialog box will appear, allowing the selection of the Export and Temp folders for the new case. By default paths to the Export and Temp folders within the default EnCase installation folder, C:\Program Files\EnCase6, are displayed. The investigator should change these paths to those specific to the case to segregate case data.

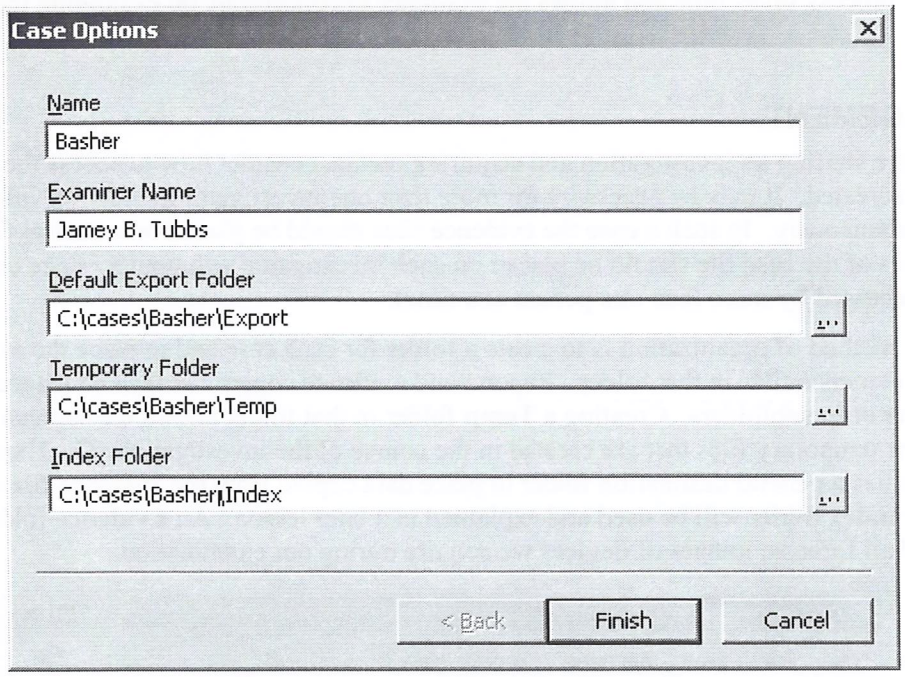

Figure 1-2 Creating a new case

Browse to the folders that you created for this case, then click on **OK**.

Next select **File→Save** or click on the **Save** icon on the toolbar. Navigate to the appropriate folder and enter a name for the case. Click on **Save** to save the new case file.

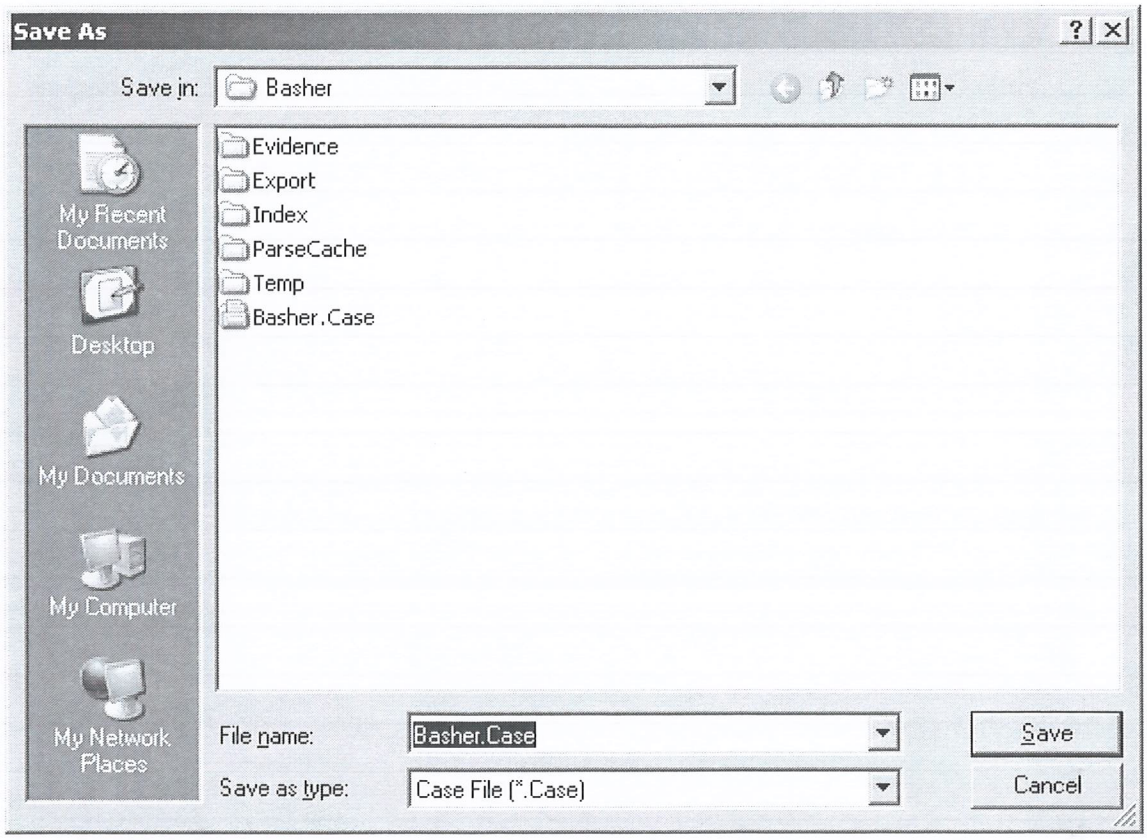

Figure 1-3 Saving a case

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

The **Case Options** tab can modify the case information entered above.

The **Global** tab allows various features to be changed, including Date and Time Display and the Auto Save Feature, picture, and timeout options.

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.

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 **EnScript** tab allows control of effects on EnScript® programs on data.

The **Storage Paths** tab provides the ability to set the paths to where .INI configuration files are stored. They can be stored in a common area accessible to all examiners and can be read-only.

The **Enterprise** tab is used strictly by EnCase® Enterprise users.

Notes