Georgia State University
CIS 8630 Business Computer Forensics and Incident Response

Workshop Protocol

Forensic Reporting with EnCase

David McDonald and Richard Baskerville

Acknowledgement:
Parts of this protocol are based on

Quick Start Training Manual for Education Distribution revision 4.0 Copyright 2003 guidance software

And

Encase 7.04 User's Guide Copyright 2012 Guidance Software. Used with permission from Guidance Software.

Version 4.1
22 September 2013

Department of Computer Information Systems
35 Broad St., NW. POB 4015
Atlanta, GA 30302-4015
USA

Table of Contents

Bookmarking for Reports 1
Lab Preparation 1
Overview 1
Sweep Bookmarks for Data 3
Sweep Bookmarks for Documents 5
Bookmarks for Email 8
Notable Files Bookmarks 9
Device and Folder Bookmarks 10
Table View Bookmarks for Deleted Material 11
Organizing Folders and Comments 14
Creating an Introductory Folder 14
Case Overview 15
Executive Summary 16
Validation 16
Recovery 17
Chain of custody 17
License statement 17
Examiner Qualifications 17
Using Report Templates 19
Report Template Structure 19
Linking Bookmarks to Report Templates 21
Viewing a Report 22
Formatting Report Templates 23
Configuring Section Body 24
Configuring Paper Layout 24
Margins 25
Customizing Headers and Footers 25
Report Styles 26
Modifying Report Template Formats 28
Localization of Report Layout 29
Editing Report Object Code 29
Example: Changing Template Contents 29
Organizing Bookmarks Content 31
Saving the Report 32

Protocol Notation

In the workshop protocol that follows, an arrow (→) at the beginning of a paragraph denotes an instruction that the participant should execute as part of their activities during the workshop.

Bookmarking for Reports

Lab Preparation

In this exercise, you will be using the same evidence file as used in the in-class tutorial.

- → Start a new case
- → Use the "EnCaseWrkShp4E.E01" found in the C:\Dayspace\Lab Evidence Files folder
- → Name this case, "Lab 1"
- → Make sure you confirm the MD5 hash value with the EnCaseWrkShp4E
- → Add to this case the raw image, "WrkShpFlppy1.dd."
- → Once the raw image is in the case, follow the instructions from the first tutorial to acquire the image and name the evidence file, "Lab1 Floppy."
- → Verify the MD5 hash value for the "Lab 1 Floppy" with the "WrkShpFlppy1.dd_audit.log" file in Dayspace.
- → Again, following the procedure in the prior tutorial, recover and deleted folders from the Lab1 Floppy

In this assignment, many of the steps will be similar to those you did in the in-class tutorial. Some tasks are purposely identical. Others are slight variations of what you've already accomplished in-class. The emphasis in this lab will be on bookmarks (and then creating a report).

Bookmarks have two purposes. They provide the basis for annotating evidence as it is found. They can also be exported directly into reports. Because of this export capability, much of the report construction can be developed in EnCase, leaving only minor formatting and organizing tasks for web page or document editing tools.

Overview

The final phase of a forensic examination is reporting the findings, which should be well organized and presented in a format that the target audience understands. EnCase reporting capabilities, include:

- Reporting templates you can use as is or modify to suit your needs.
- Capability to control a report's format, layout, and style.
- Ability to add notes and tags to a report.

Reports in EnCase consist of three parts:

- Bookmark folders where references to specific items and notes are stored.
- Report templates that hold formatting, layout, and style information. A report template links to bookmark folders to populate content into a report.
- Case information items, where you can define case-specific variables to be used throughout the report.

In EnCase, as you work on a case, you typically discover files, portions of files, and other items of interest and save them as bookmarks. The report template links to bookmark folders to populate content into the report. Bookmarks are saved in folders in the case file. When you create a new case and apply one of the supplied case templates, EnCase provides bookmark folders by default. As an example, the basic template provides these folders:

- Examiner Notes
- Documents
- Pictures
- Email
- Internet Artifacts
- Other Findings

You can also create your own folders. For example,

→ Open the case you created in the "Introduction to EnCase" Workshop, From the Home Tab, choose View Bookmarks. Notice the default folders are present below, *plus* the folder "Types of Literature Read" created for the Table Bookmarks during the "Introduction to EnCase" Workshop. In this lab, recreate this bookmark folder.

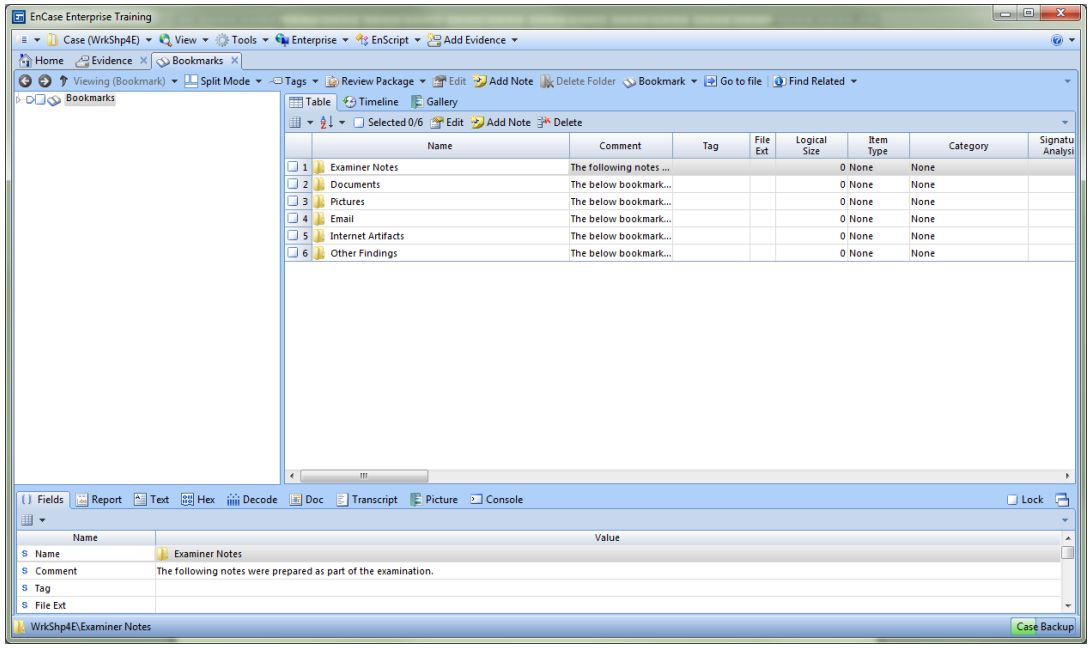


Figure 1. Bookmark Folders

→ Right-click on the Bookmarks root in the Tree pane.
→ Select "New Folder"
→ Right-click on the generically named folder and choose Edit
→ Name the folder "Types of Literature Read"

Recall from the introductory workshop that you can bookmark data and save the bookmark in a folder by selecting the content you want from any tab (for example,

Entries, Records, or Search Results) and click Bookmark on the tab toolbar. For example, replicate what was done in-class:

Sweep Bookmarks for Data

→ As you did in the Encase tutorial, create a sweeping bookmark for "Uses for Dry Ice"

→ In the Comment area, enter: "Evidence for creating a dry ice bomb in the file Dc555.doc" Click OK. (this is what we did in-class)

→ To change this comment, right click on the bookmark comment, select Edit, and replace the comment as follows (modify what we did in-class):

> "One of several copies of the Anarchist's Cookbook found on the thumb drive. The cookbook contains instructions for making simple, delayed action time bombs by sealing dry ice in a plastic container."

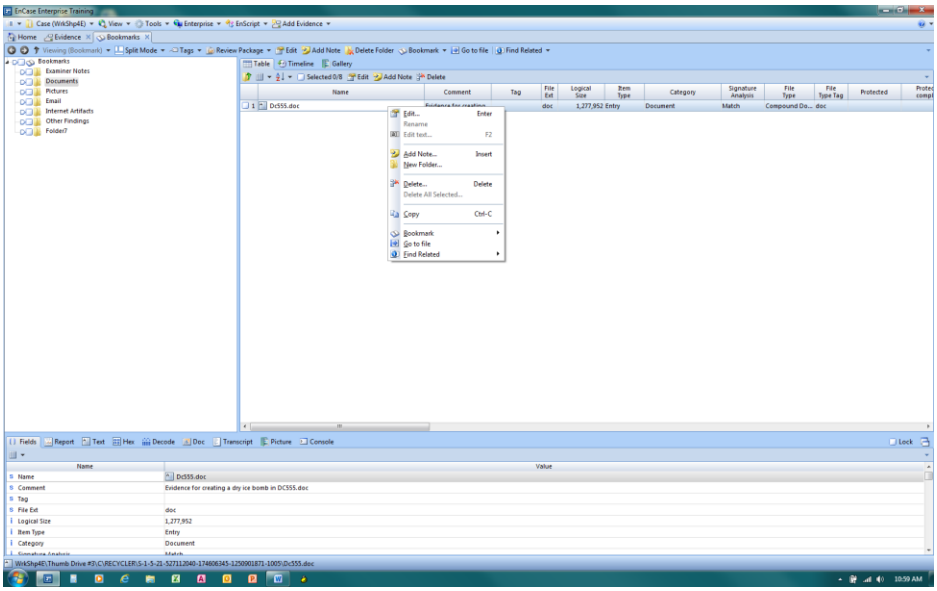


Figure 2. Editing a bookmark – Add/change useful comments to data.

Another Example

→ Select View, Search to bring up the index search tab. Enter "mcdonalds" into the index field and "search using the criteria on the current tab" (green right pointing triangle). This is an alternate method to activate an Indexed Search.

→ Change the Text Style in the View pane to "Western European (Windows) – Line Breaks (120)

→ In the Chaos Cookbook, Select the first few lines from "How to Terrorize McDonalds" select the text containing the first paragraph (See figure), and click **Bookmark Raw text** on the tab toolbar.

→ In the dialog box, add the comment "Terrorizing McDonalds" and set the Destination Folder to Documents. Click OK.

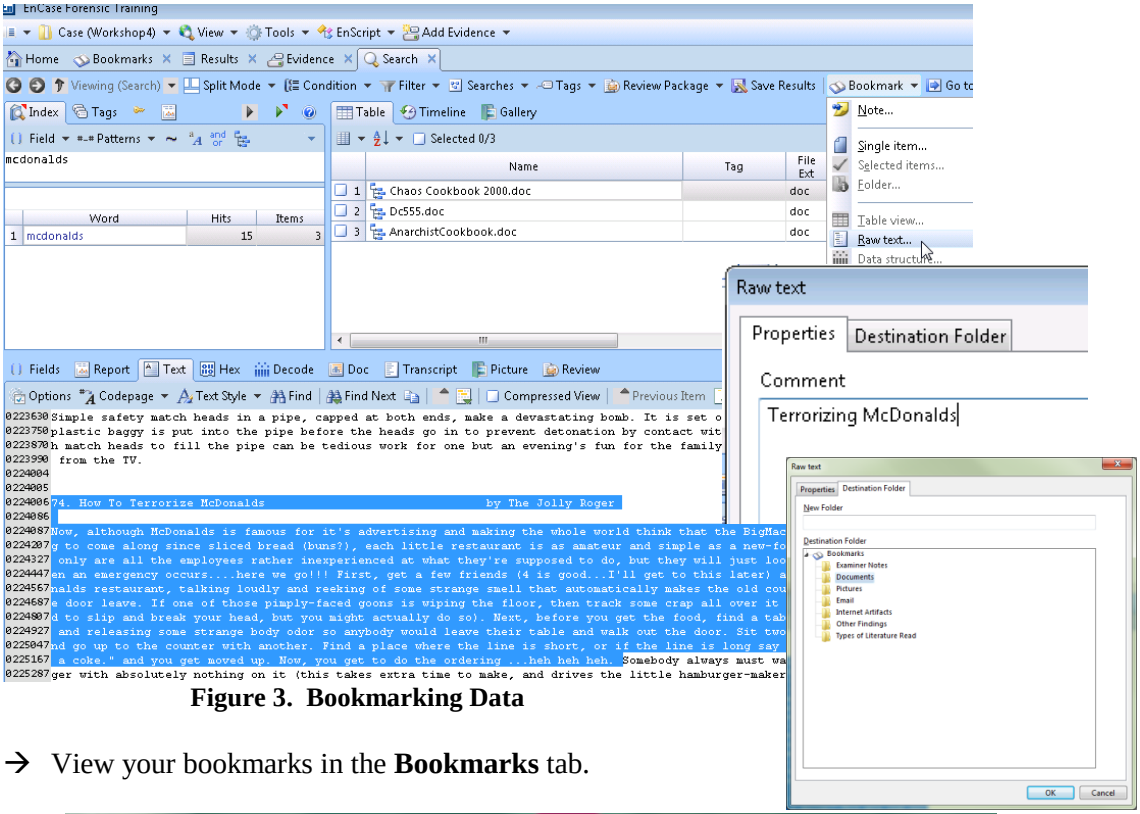
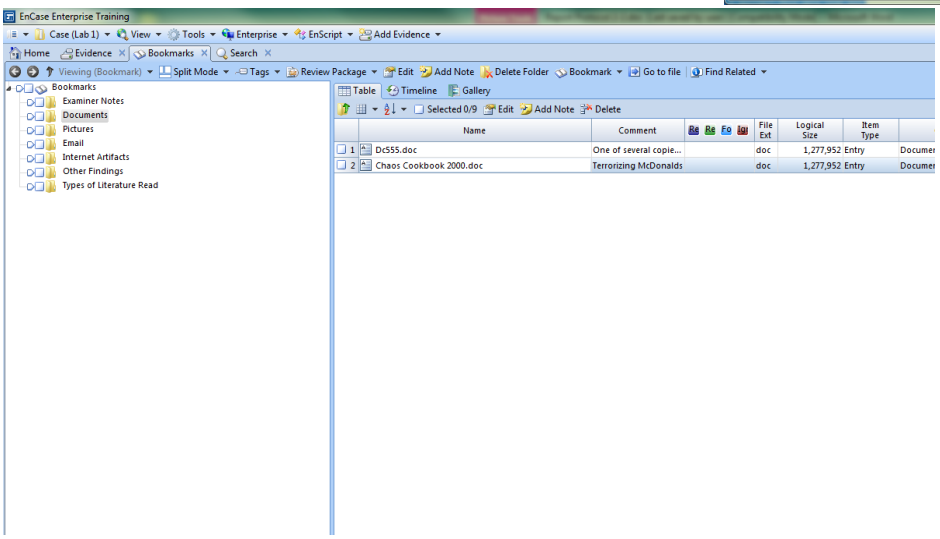


Figure 3. Bookmarking Data

→ View your bookmarks in the **Bookmarks** tab.



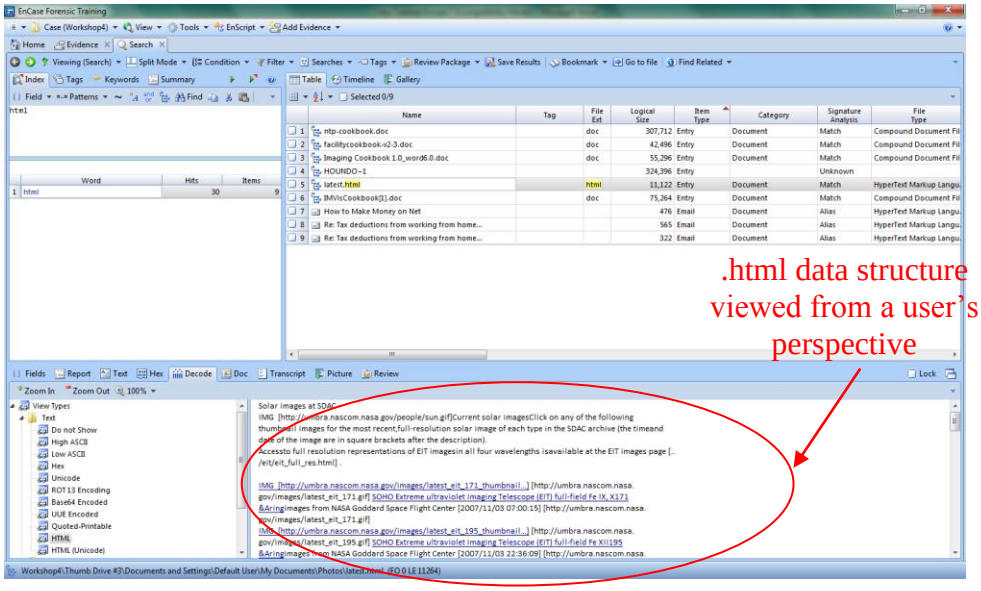
Data Structure Bookmarks

Data structure bookmarks mark items such as a Windows partition entry, a Unix text date, or encoded text. Data structure bookmarks is really a misnomer. A sweeping bookmark is generally used but the text which has been highlighted is meaningless. Thus, the investigator can use Encase's "Decode" capability to interpret the data and present it in a more meaningful format.

This section describes one example of creating a sweeping data structure bookmark on an html data item. Some common data structure files, such as all graphics files, are automatically interpreted by Encase. However, there are many other data structures for which Encase can easily analyze and interpret.

To create a data structure bookmark:

- → If the **Search tab** is not opened, go to the **View menu** and select **Search**.
- → On the **Search tab**, select **Index**. **Enter** the term "html" to quickly search for an html data structured file
- → Select "Latest.html" in the Table pane.
- → Examine the file content in the View pane using the **Text** tab. Most users will recognize this format as an html encoded text file.
- → **Sweep or Highlight** the entire file contents (or use a CTRL-A to select all).
- → Click the **Decode** tab. The View Types tree displays inside the left part of the View pane.
- → Since the examiner is investigating html data in this example, expand the **Text** folder and click on the "html" option.
- → The **html** option yields a satisfactory representation of the data, as shown in the figure below.



→ To bookmark the data, right click the **interpreted html** code in the View pane, and select **Bookmark** > **Data Structure** *or* on the menu bar, click **Bookmark** > **Data Structure**.

→ In the Data Structure dialog, type "Translated HTML Code" in the **Comments** box and click the **Destination Folder** tab.

→ In the **Destination Folder** box, click the **"Internet Artifacts"** bookmark folder to store this data structure bookmark.

→ Click **OK**.

Sweep Bookmarks for Documents

Some formatting from word processing and other documents can be preserved by **exporting the data**.

→ Select the Bookmarks tab (if not shown, use the View menu to show the tab).

→ Highlight the Dc555.doc file in the Table pane.

→ In the View pane, scroll to the top of the document. Then scroll down a few lines, noticing the header indications that this is a Microsoft Word 6.0 Document.

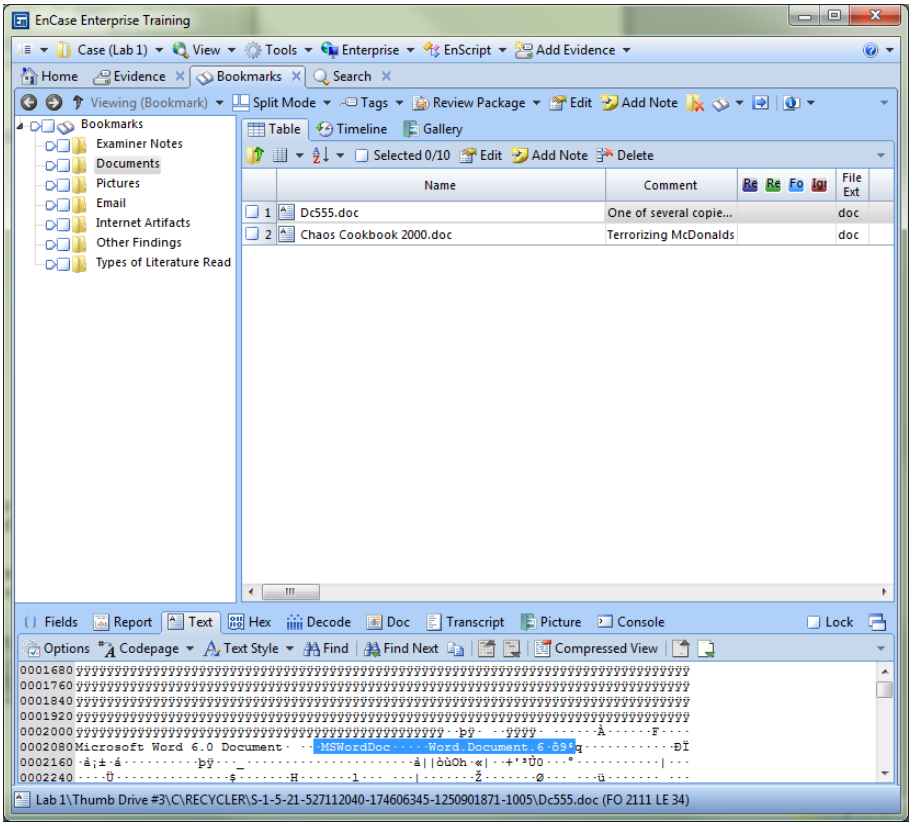


Figure 2. Discovering Document Types.

→ Select "DOC" as the display mode in the bottom pane. "DOC" view will also work with many other formats including XLS, PPT, and PDF files. Note the name of the file (Dc555.doc).

→ Right click on the bookmark, and choose "Go to file" In the Tree View (upper-left pane), note that Dc555 is located in the Recycler. This indicates the document was in the user's Recycle Bin.

→ Highlight the title, author and table of contents in the display window. Right-click on the highlighted area. Notice there is no choice for a bookmark while displaying DOC files in the View pane.

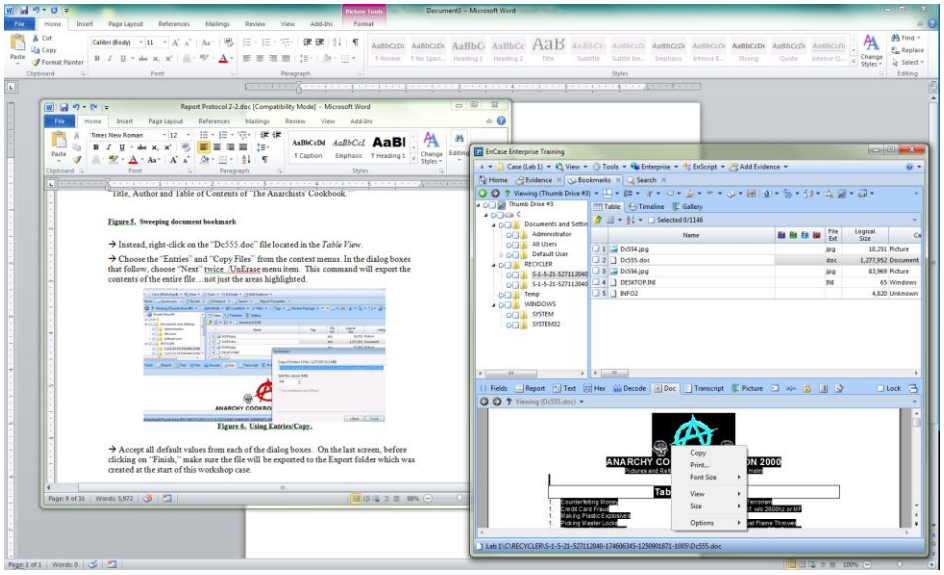


Figure 3. Sweeping document bookmark (can't be done)

→ Instead, right-click on the "Dc555.doc" file located in the *Table View*.

→ Choose the "Entries" and "Copy Files" from the context menus. In the dialog boxes that follow, choose "Next" twice /UnErase menu item. This command will export the contents of the entire file…not just the areas highlighted.

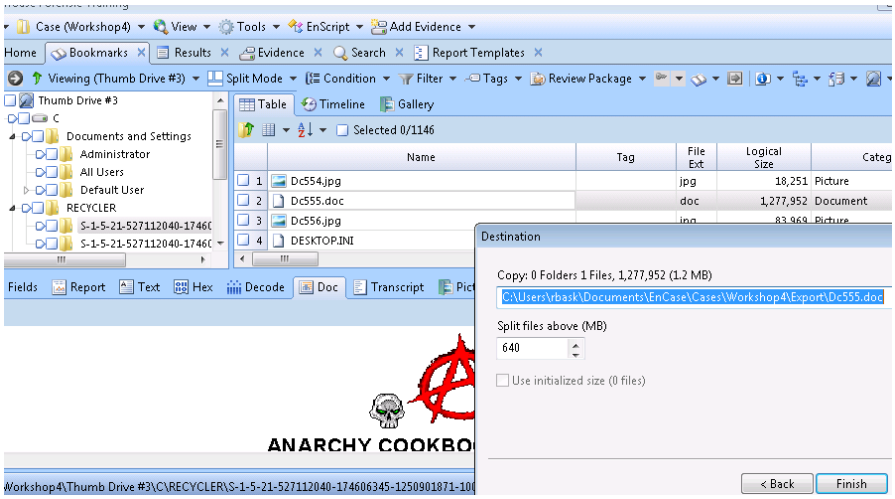


Figure 4. Using Entries/Copy.

→ Accept all default values from each of the dialog boxes. On the last screen, before clicking on "Finish," make sure the file will be exported to the Export folder which was created at the start of this workshop case.

The exported file is a read/write file. You can highlight the necessary evidence and the use a Notes Bookmark to add the selected evidence to your Bookmarks.

IMPORTANT NOTE: You *must include how and why* you exported the data to get the bookmark for your report. The exported file was modifiable. Thus, opposing counsel in a court of law may question the validity of this data. Using this methodology should only be done if creating a Notable File bookmark would create an inordinate amount of useless data to the final report. Thus, in this example, we are only showing the Table of Contents. The report should indicate that the original file can and will be presented if necessary

.

Bookmarks for Email

→ Using the techniques from the introductory tutorial, search for "dry ice" and notice the item type of result number one "Email". Select the Report tab on the View pane at the bottom. Notice the message itself is not displayed in the bookmark's report view.

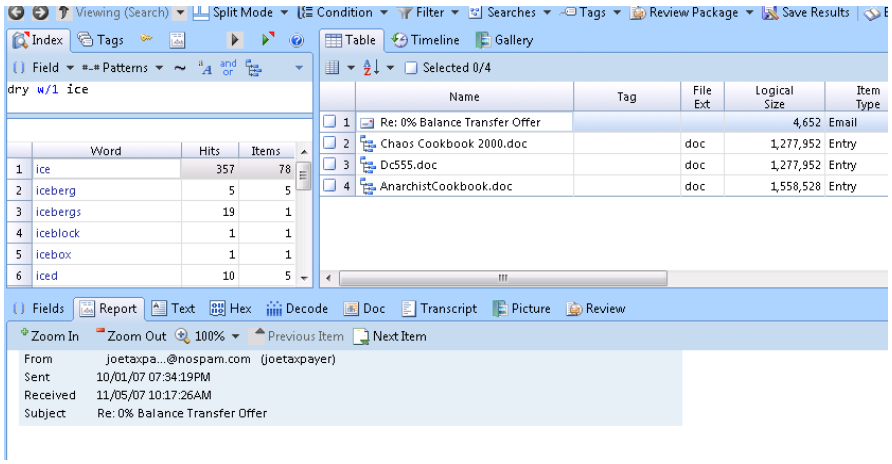


Figure 5. Email in an indexed search.

→Right click on the bookmark in the Table pane and select "Bookmark" and "Single Item" from the context menu. Include the comment, "Reference to Yew Alley & Dry Ice in Email." Set the Destination Folder to "Email". Click OK

→Select the "Doc" tab in the Display pane. Highlight the text of the message and create a sweeping bookmark for this text. Include the comment, "Text from email of 10/01/07". Set the Destination Folder to "Email". Click OK

Notable Files Bookmarks

→ Select Evidence … Entries and select "Folder 1" from the recovered files on the Workshop Floppy disk image. Right click on NE Dictonary.Doc and select Bookmark Single item. Add a comment

> "Nigerian English" Dictionary. Perhaps related to 419 Scam."

→ Choose Bookmarks tab and review the bookmarks (delete any extras or mis-tries by right clicking on the bookmark and choosing delete).

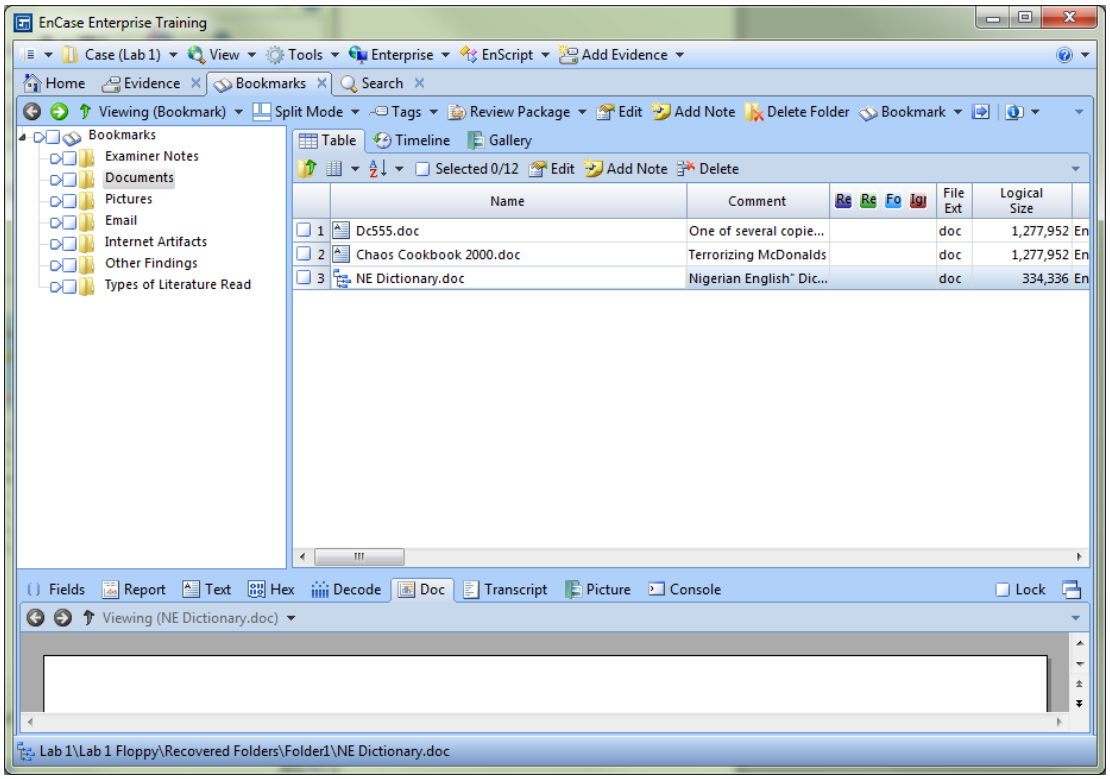


Figure 6. Sample bookmarks.

Device and Folder Bookmarks

→ Choose Evidence Entries and Thumb Drive #3. Right click on Drive C. Select Bookmark … Folder.

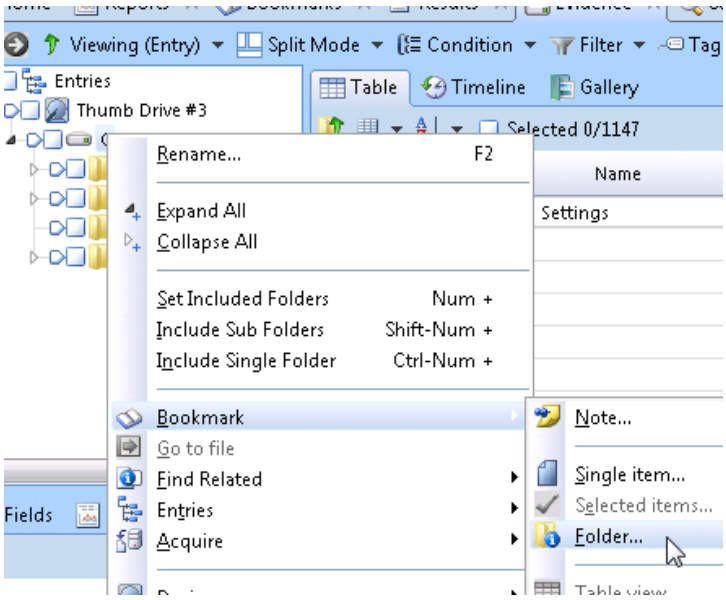


Figure 7. Creating a folder bookmark.

→ Name the bookmark "Thumb Drive #3 Drive C Folder Structure" and select Next.

→ Select the root "Bookmarks" folder as the Destination Folder and enter "Device Folder Structures" as the New Folder name. Click Next.

→ Check "Show Nodes" and then click Finish.

→ Repeat this process and bookmark the device and folders in the Workshop Floppy Disk Image. Place this bookmark in the Device Folder Structures folder created in the previous step.

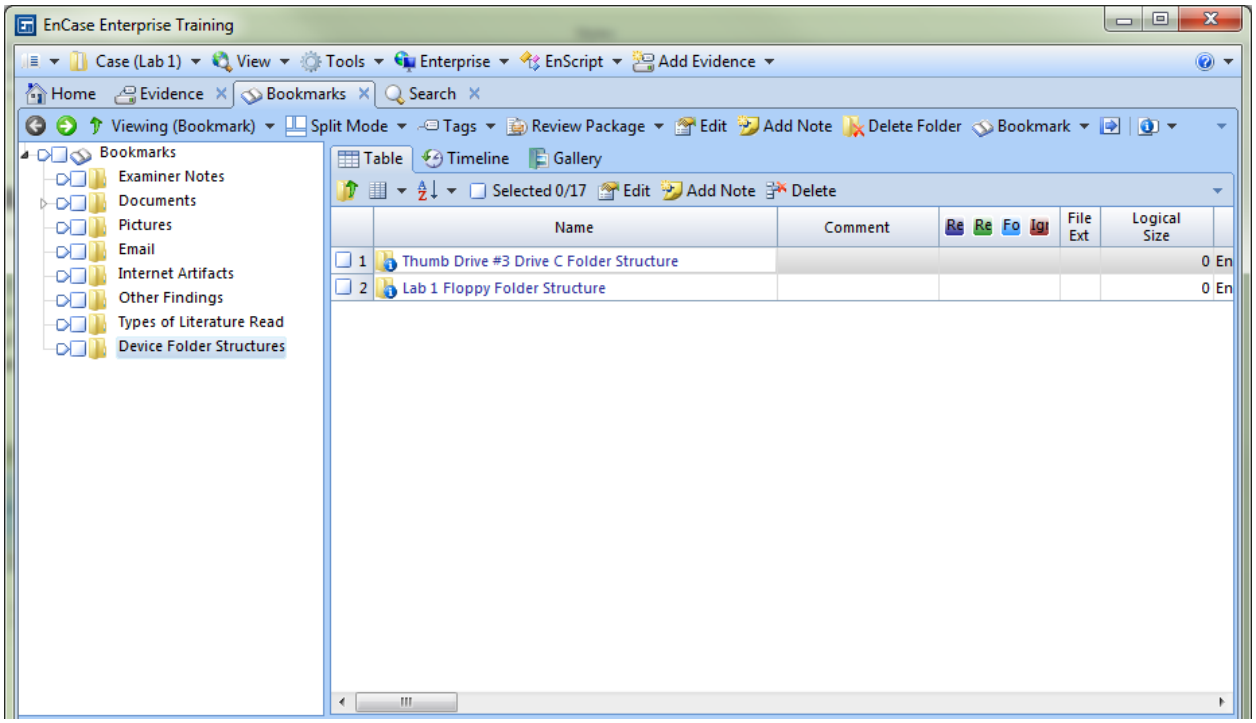


Figure 8. Data and folder bookmarks.

Table View Bookmarks for Deleted Material.

→ Select Evidence … Entries and go back to the Thumb Drive #3 evidence. Use the left Tree pane to navigate to the My Documents\Terrorist directory. Note that all entries have been deleted.

A Table View group bookmark can be used to create a meta-data table for any files that have been selected. These bookmarks are typically located within a separate bookmark folder. The structure enables a group of files to have a single comment and to be easily created.

→ Check the Terrorist folder, and note that all files in the folder have been selected in the right Table pane. Right click on any file in the table and choose Bookmark … Table View and name the Bookmark "Deleted Files in Terrorist Directory". Add the following comment and click Next.

> "All files in the terrorist subdirectory had been deleted. These included multiple versions of the Anarchist Cookbook and many images of bombs and explosions."

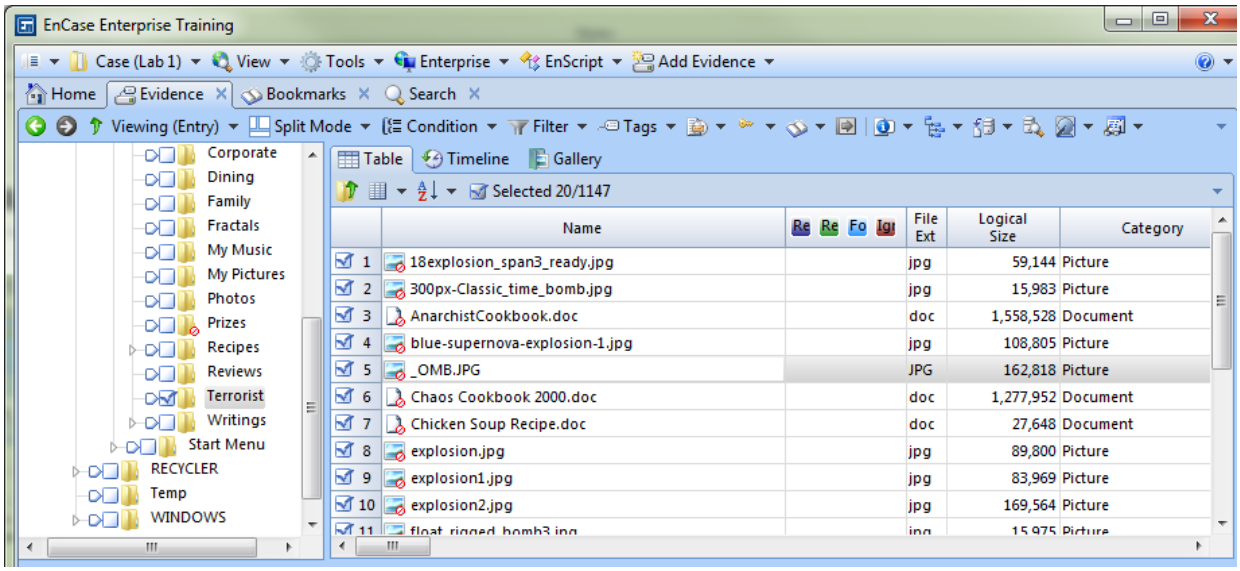


Figure 9. File group Table View bookmark.

→Select "Documents" as the Destination Folder and enter a New Folder name "Deleted Terrorist Documents Attributes". Select Next.

→Place a check on the following columns for the table view: Name, File Ext, Logical Size, Category, File Type, Last Accessed, Last Written, File Created. Click Finish.

Multiple Notable File Bookmark (Selected Items) for Deleted Material

→ Uncheck the Terrorist Folder.

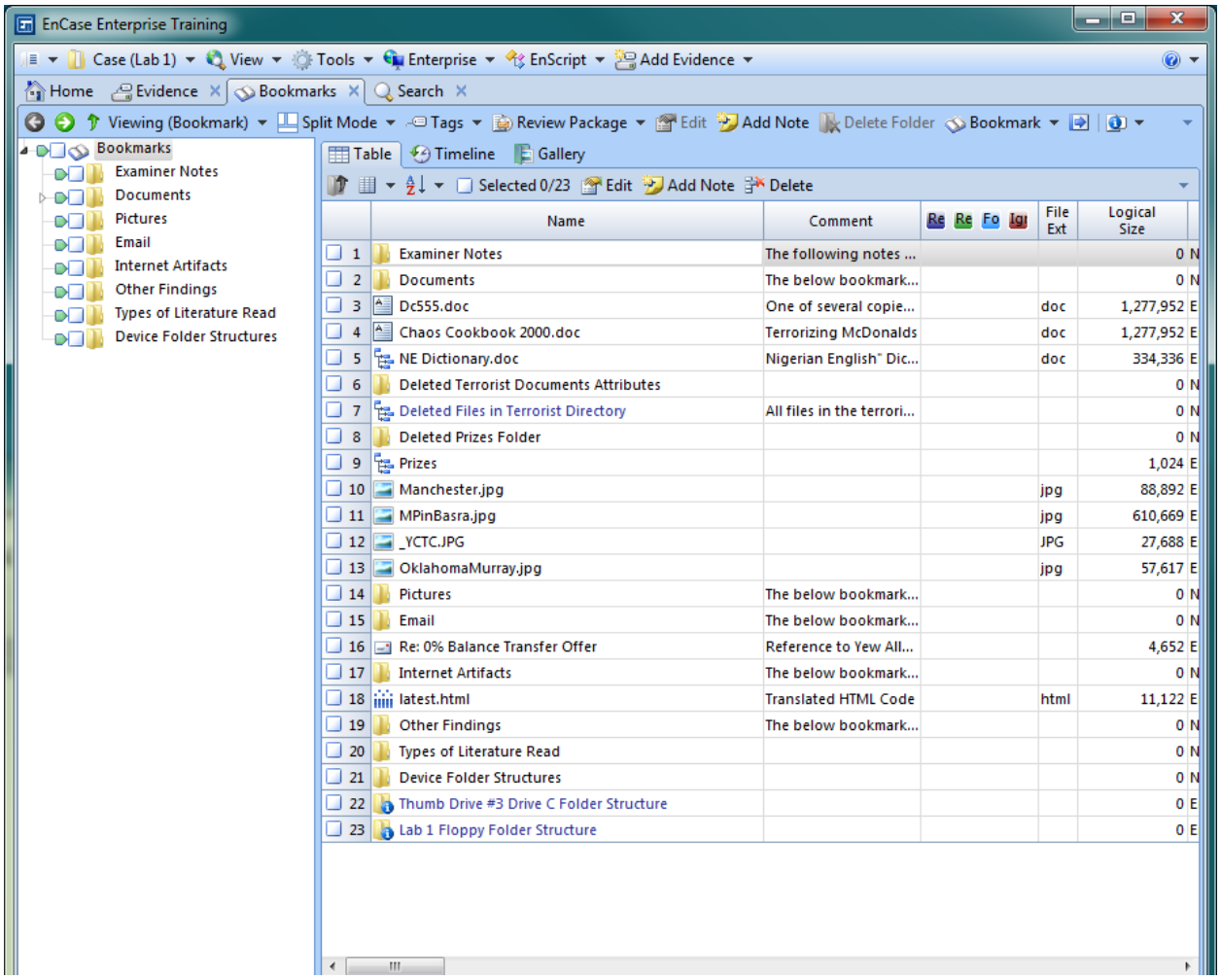
→ Check the Prizes folder in the Tree pane.

→ Right-click on any file in the Tree pane and choose Bookmarks->Selected Items…

→ Highlight the Pictures Bookmark Folder and name a new folder "Deleted Prizes Folder" as the Destination Folder in the Bookmark dialog box.

Bookmarks should now include at least two data bookmarks (one on Dry Ice and one on McDonalds), two single notable file bookmark or selected item bookmark (NE Dictionary.Doc and the Yew Valley email), one multiple notable file or selected items bookmark folder (Deleted Prizes Folder), one data structure bookmark (latest.html), one table bookmark (Deleted files in Terrorist Directory), two folder information bookmarks

(Thumbdrive C and Lab 1 Floppy). The figure below uses the "Set Include" marker to display all bookmark folders and contents in the Table pane.



Organizing Folders and Comments

Forensic reports follow a fairly standardized outline. In this lab, the bookmark folders must be created *before* any attempts at modifying the Report Template. Some of the folders have been created in prior steps of this lab. Others will have to be created as you continue with this lab. Type in the sample data as directed below.

We will use the following bookmark folders for a forensics report of this evidence:

1. Introduction
    a. Author: Report Prepared By
    b. Client: Report Prepared For
    c. Case Overview
    d. Executive Summary: Results
2. Device Folder Structures
3. Examination Findings
    a. Dry Ice
    b. Nigeria
    c. Terrorism, Bombs, and Explosions
4. Forensic Process
    a. Validation
    b. Recovery
    c. Chain of custody
    d. License statement
    e. Examiner Qualifications

Creating an Introductory Folder

Introductory material can be presented through Note Bookmarks

→ Choose the Bookmarks Tab. Right click on "Bookmarks" in the left Tree pane and select "New Folder".

→ Highlight the new folder in the Tree pane, right-click and choose Edit.

→Rename the new folder "Introduction".

→Right click on the Introduction folder and choose "Add Note". Name the new bookmark "Prepared By" and enter the following Comment:

Your Name
35 Broad Street
Atlanta, GA. 30033

→Right click on the Introduction folder and choose "Add Note". Name the new bookmark "Prepared For" and enter the following Comment:

Duke Buntline
RollingCase Corporation
Assignment in Forensics Workshop

(Be sure that you press “Enter” after the last line in this comment. Make sure the Destination Folder is set to “Introduction”.

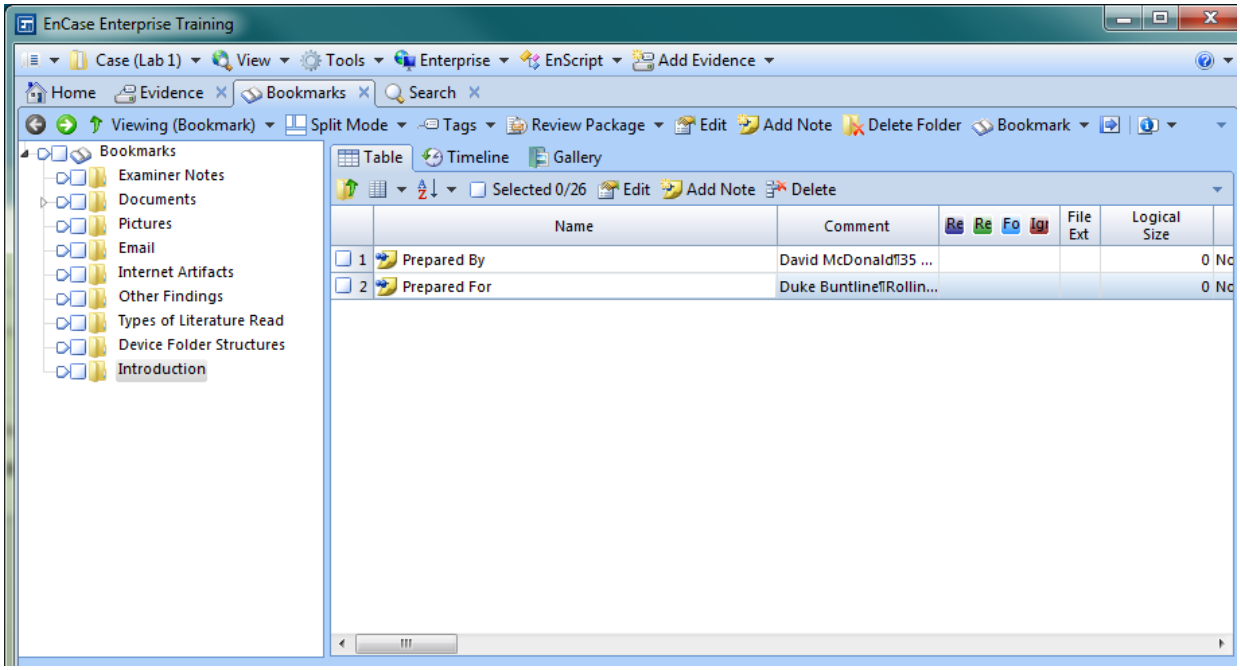


Figure 10. Creating Typical Bookmark Entries for the Final Report.

→ In a similar manner, create the following Note Bookmarks for the Introduction folder.

Case Overview

On November 10, 2015, Duke Buntline, head of security for RollingCass Corporation, requested forensic examination of two items of computer meda: one thumbstick and one floppy diskette. Mr. Buntline reported that the media had been removed from the office of Mr. Dan Kojak, a computer information systems intern with the company. Mr. Buntline suspected that Kojak was operating a 419 scam among RollingCass employees using his assigned computer workstation, a violation of company policy. The investigation was hampered by the destruction of the hard drive of Kojak’s computer workstation. It appeared to have been was destroyed by a powerful acid, perhaps nitric, set to operate as a timed internal pipe bomb, perhaps using dry ice as a timer.

Mr. Buntline asked that the media be examined for any evidence of time bombs, pipe bombs, dry ice, or “419 Nigerian” scams, or any other notable evidence of suspicious activity by Kojak.

Executive Summary

The thumb drive contained several copies of "The Anarchist Cookbook" which included many references to both pipe bombs and time bombs. There were also references to the construction of time bombs using dry ice. The cookbook includes instructions for constructing such devices. There were also many photos of explosion scenes. All of this evidence was in a subdirectory named "Terrorist", and these files had been deleted. The files were recovered from free space or the Recycler.

The thumb drive also contained a collection of cook books, recipes, photos of food, and text files of books and literature.

There was also one email message with a reference to dry ice and a "yew alley". This may have been a reference to a "yew alley" mentioned in one of the literary works ("The Hound of the Baskervilles"), but the meaning of this connection is not clear to the examiner.

The floppy diskette had been formatted, but we recovered one directory containing a small Danish-English dictionary and a dictionary of "Nigerian English". There is no obvious relationship between the material on the floppy and the material on the thumb drive, although the latter dictionary could be somehow related to the 419 scam.

→ In the Tree pane, select the Introduction folder and drag it to the top of the tree under "Examiner Notes" bookmark folder.

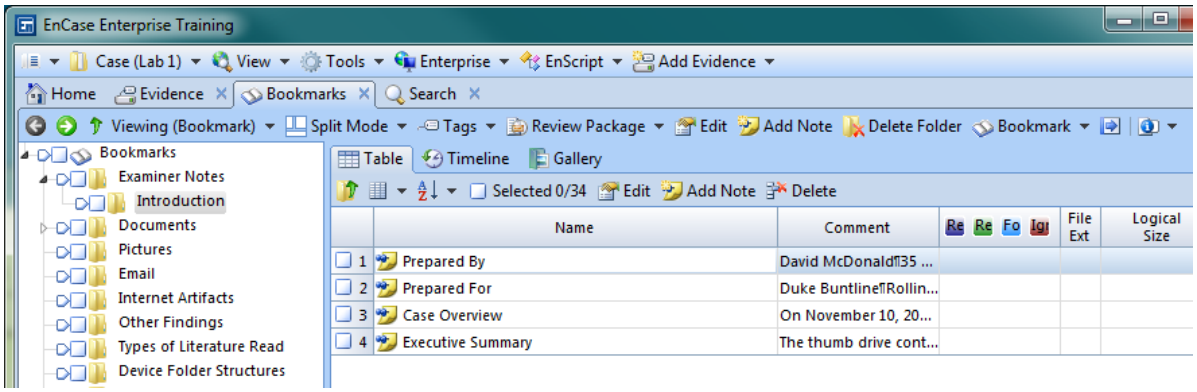


Figure 11. Relocating a Bookmark Folder

→ Repeat this process to create a Bookmark folder named "Forensic Process" at the bottom of the folder list. In this folder add five Bookmark Notes:

Validation

The evidence item, original memory stick, was attached via a write protection block o a computer operating under Windows XP, and imaged using the FTK Imager as an EnCase Evidence file. The MD5 hash of the original device was calculated in this process. An image of this memory stick was then copied to a Virtual Computer operating EnCase Forensics Analysis software. Upon completion of the transfer process, EnCase was again

used to verify the integrity of the evidence file and calculate a MD5 Hash for the evidence and it was verified that the evidence image was unchanged by the imaging or the transfer process. The original memory stick was then removed from the computer and stored in a locked repository.

The evidence item, the floppy diskette was write protected, read by a computer operating under Windows XP, and imaged as a simple dd image file using the FTK imager. The MD5 hash of the original floppy volume was calculated in this process. attached via a write protection block o, and a hash calculated md5deep. An image of this memory stick was then copied to a Key Computer Service hard disk drive using dd for windows)..

The image of this diskette was then copied to a Virtual Computer operating EnCase Forensics Analysis software. Upon completion of the transfer process, md5deep was used to calculate a MD5 Hash for the image and it was verified that the evidence image was unchanged by the imaging or the transfer process. This evidence was then loaded into EnCase, acquired by EnCase, and EnCase again used to verify the integrity of the evidence file and calculate a MD5 Hash for the evidence. It was verified that the evidence image was unchanged by the imaging, transfer or acquisition process. The original diskette was then removed from the computer and stored in a locked repository.

Recovery

Encase automatically recovered the files deleted from the original thumb stick, most notably all files in the directory “Terrorist”. There was a single outlook pst (personal folders) file, unencrypted, on the thumb drive. The structure of this file was restored by means of an EnCase keyword search.

The floppy diskette appeared to be blank, however, applying the “Recover Folders” procedure of EnCase recovered one folder, indicating that the floppy was likely formatted.

Chain of custody

Nov 10, 9.50 am. Smith received the two evidence items from Buntline at his offices in Broad St.

Nov 10, 11.30 am. Smith seals the two evidence items in a tamperproof bag and locks the parcel in his evidence repository safe in his offices in Broad St.

See the Chain of Custody Form attached to this report for further details

License statement

All software utilized is licensed to, or authorized for use by, the examiner.

Examiner Qualifications

Buck Smith is a forensics examiner trained at Georgia State University, in its information security and its computer forensics courses. He has two years of experience as a computer specialist. Expecting to graduate in 2015, Smith will hold a Degree in Computer Information Systems.

On completion of the construction of the organizing bookmarks, the bookmark tree should be similar to:

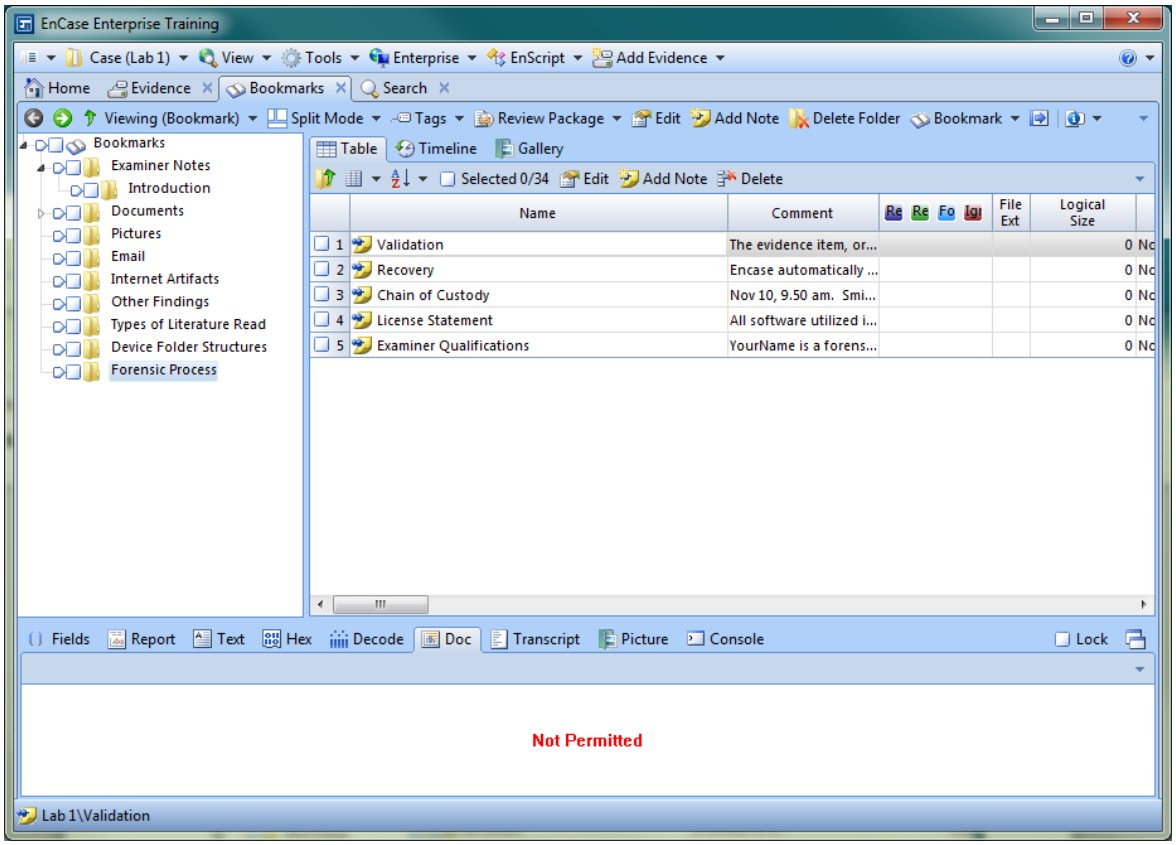


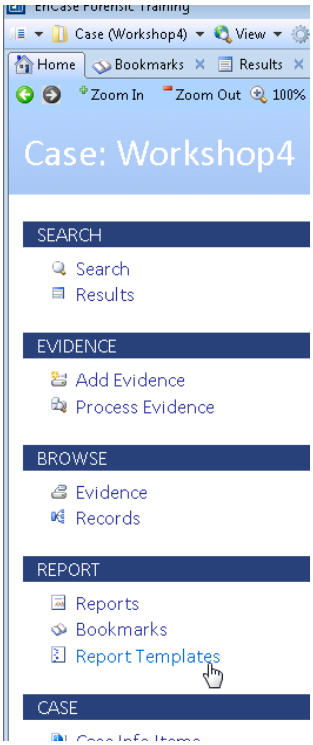
Figure 12. Complete set of bookmarks.

Using Report Templates

A report template is one component of a case template. Each default case template includes a customizable report template. Different case templates can contain different report templates, and each of these templates is completely customizable. In addition to the report template, each case template also includes bookmark folders that are referenced in the report.

Besides the default templates, you can define your own custom reports and save them as part of a case template.

Report Template Structure



Before viewing a report, you need a report template, or outline of what the report will look like. This structure consists of:

- Report sections: groups of similar information and formatting that provide the ability to organize your report.
- Report formatting: page layout, section design, and text styles.
- Report elements: collections of bookmarks. Bookmarks are a key element of the report structure. You do not embed bookmarks into a report template, but embed a *reference* to the contents of a bookmark folder.

To display the template, click **Report Templates** on the case Home tab:

A report component is designated as either a Report or Section, as shown in the Type column. Typically, Report components contain only formatting information for components beneath them, whereas Section components contain formatting information and Report elements for an individual section. The columns to the right of Type indicate whether a formatting option is user defined or inherited from the component above it in the template hierarchy.

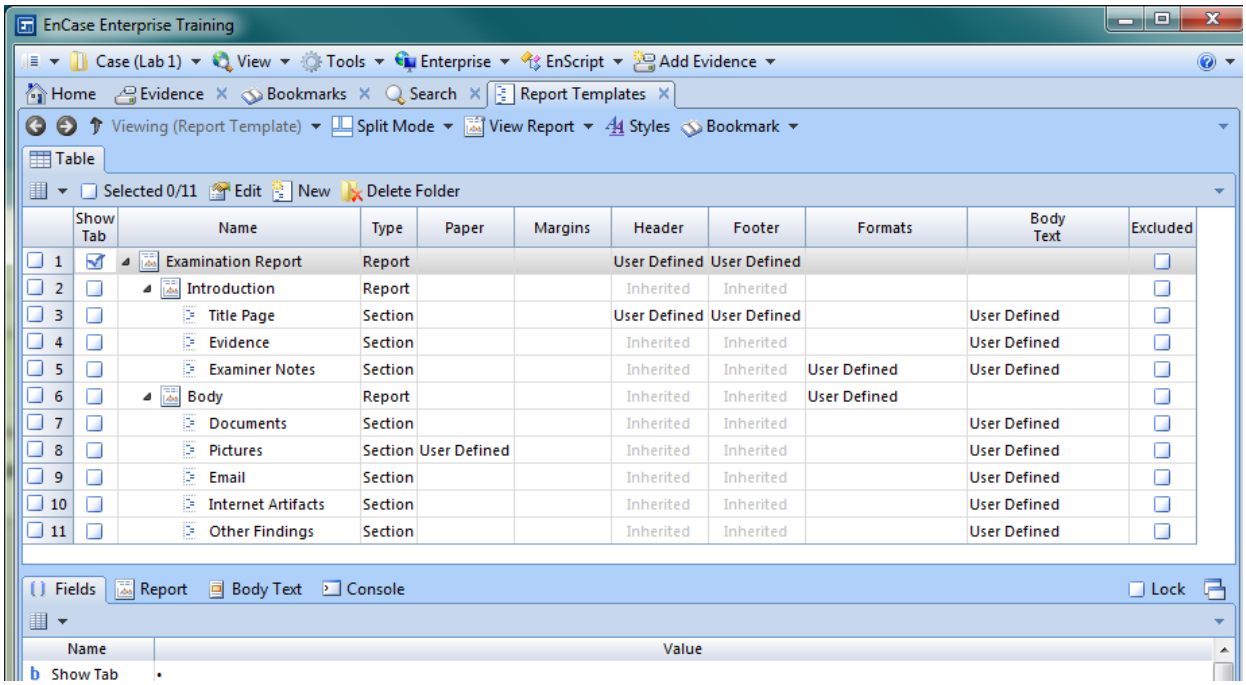


Figure 13. Reports Template Table.

To add new Reports or Sections to the template:

→ Highlight the row logically *above* the new element you want to add. In this case, highlight the row "Body". Right click and select **New** from the dropdown menu.

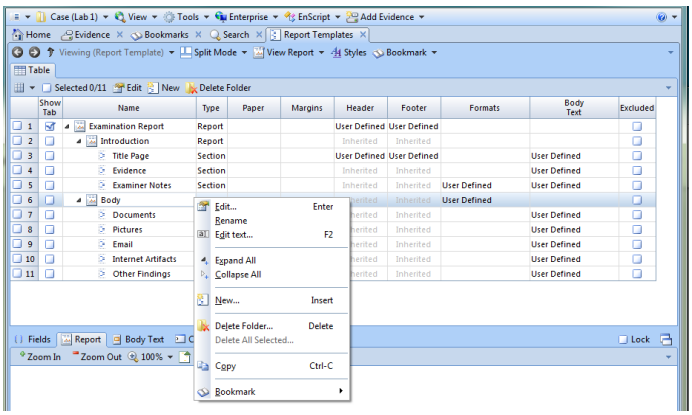


Figure 14. Adding new template to Body.

→ The New Report Template dialog opens.

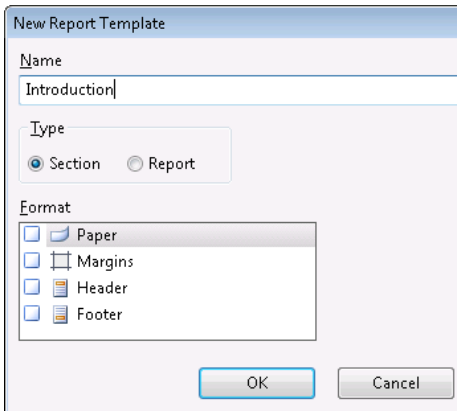


Figure 15. Naming new template.

- → Enter the Name "Introduction".
- → Select Section Type (Default).
- → Note you can customize Format styles or leave the boxes clear to use the default styles.
- → Click **OK**. The new template component displays below the row you highlighted.

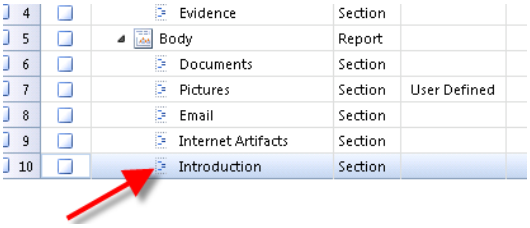


Figure 16. New section added to Body.

Note that there is both an "Introduction Section" in the "Body Report" and a separate "Introduction Report". We will be mainly working with the Introduction *Section.*

Linking Bookmarks to Report Templates

In the new section above, assume a prior created bookmark folder with data. To link this bookmark to the new Report Template section:

- → Right-click on the **Introduction** section which was just created
- → Choose **Edit** from the pop-up menu
- → Click on the **Body Text** tab
- → Click on the **Bookmark Folder** menu entry
- → Select the **Introduction** bookmark folder which was created earlier under the *bookmark* folder, "Examiner Notes"
- → Check the **Show Folders** checkbox on the upper left section of the dialog box.
- → Click **OK**, then **OK** again

This bookmark folder and all types of bookmarks located in this folder will become included in the planned report under the section heading, "Introduction."

- → Repeat the linking process for the Forensics Process bookmark folder.
- → Switch to Tree-Table view in the Report Template

- → Using the mouse to drag the report templates items in the *Table pane*, rearrange the Body sections into the following order: Introduction, Documents, Pictures, Email, Internet Artifacts, Forensic Process, and Other Items.
- → When finishing moving template items, make sure the view is switched back to Traeble. Traeble view allows viewing of the report content in the View pane.

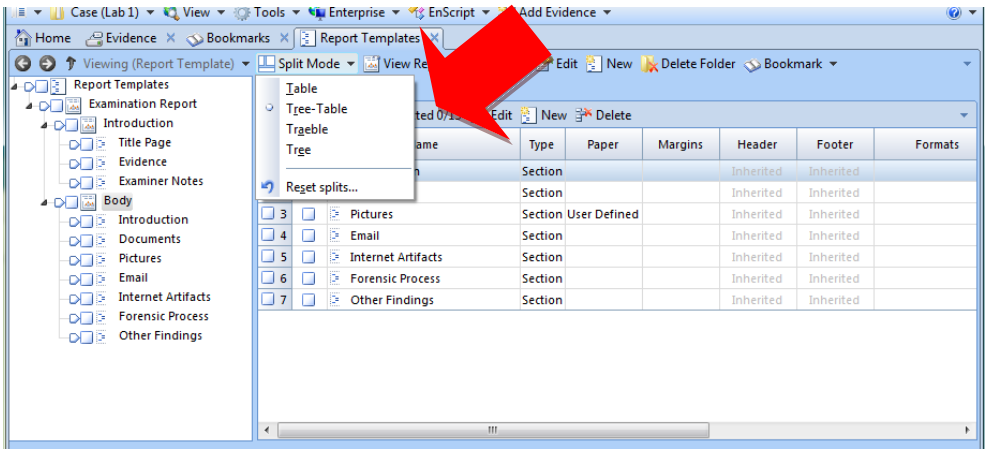


Figure 18. Reorder Body Sections – Use the Table Pane to Reorder.

To link the Device Folder Structure bookmarks to an existing *linked* template item, do the following:

- → In the Report Template, right-click on the **Evidence** *section* item in the first part of the report (make sure you are back in Traeble view.
- → Select **Edit** and click on the **Body Text** tab.
- → Place the cursor on a new line at the end of the existing program code.
- → Click on **Bookmark Folder** menu entry
- → Select the **Device Folder Structure** *bookmark folder*
- → Check the **Show Folders** checkbox on the upper left section of the dialog box.
- → Click **OK**, then **OK** again.

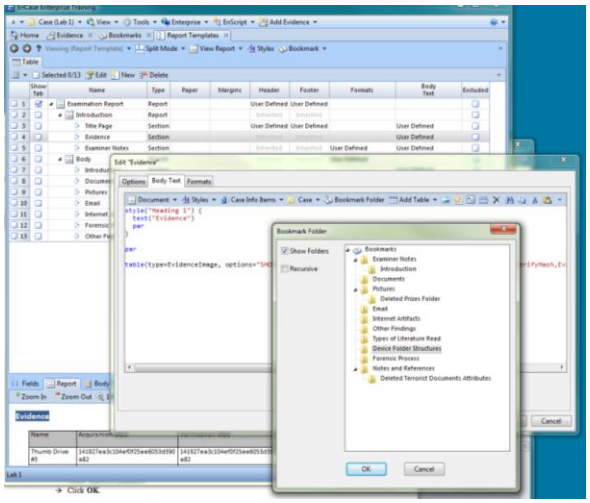
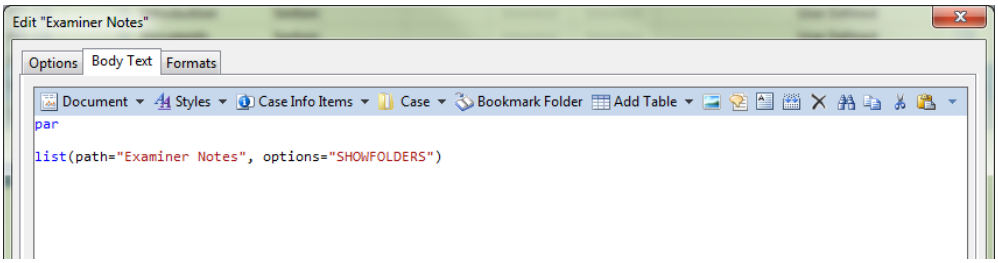


Figure 19. Modifying an Existing Template Link

Unlinking a Bookmark Folder From a Report Template

In the new section above, assume a prior created bookmark folder with data. To unlink this bookmark from the Report Template section:

- → Right-click on the **Examiner Notes** section in the Report Template
- → Choose **Edit** from the pop-up menu
- → Click on the **Body Text** tab
- → Remove the word "RECURSIVE" from the auto-generated program code
- → Make sure there are closing quotation marks and a close parenthesis marker after the word "SHOWFOLDERS"
- → Click **OK**.



Viewing a Report

To view a report:

- → In the **Report Templates** tab, click **View Report** from the tab toolbar. The dropdown menu lists all reports that have the **Show Tab** option set.

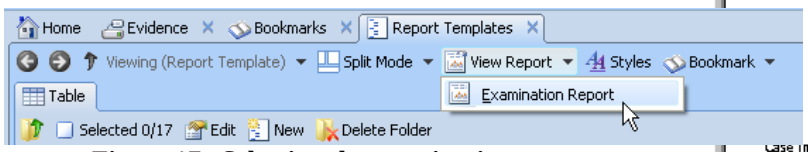
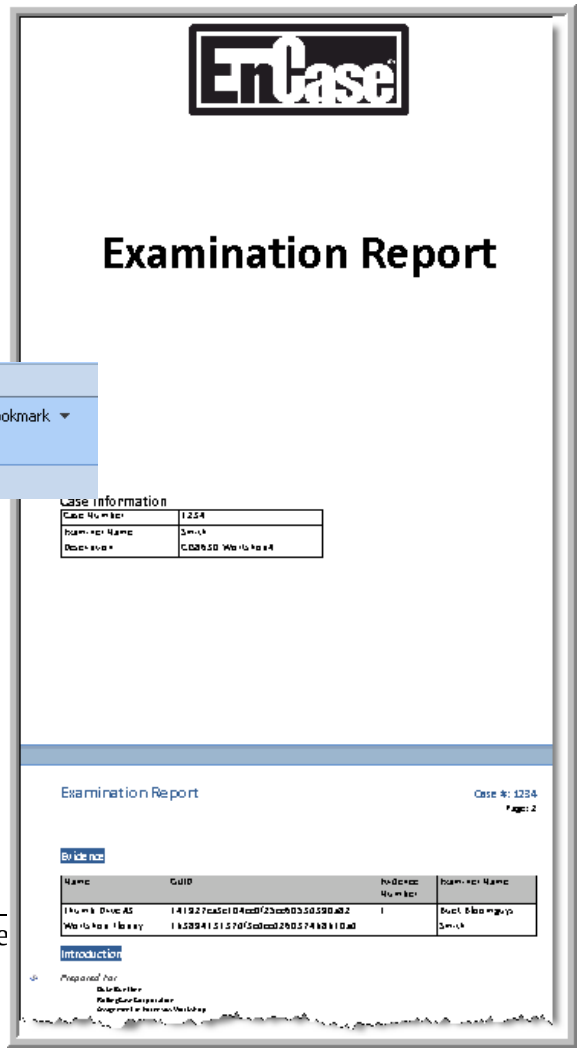


Figure 17. Selecting the examination report.

- → Select the report you want to see. The report displays in the viewer. As you browse the report notice it has superfluous material and is difficult to read.



Formatting Report Templates

A wide range of formatting options is available for customizing EnCase reports. Guidance Software recommends using the default case templates to start, then customizing them as needed.

Report templates follow a hierarchical tree to simplify formatting. Report sections inherit formatting options from above so that changes to formatting only need to be made in one place.

You can customize these elements:

- Section Name: Used for organizational reference in the template only and does not populate the report.
- Paper: Includes orientation and size.
- Margins: Set values for top, bottom, left, and right margins.
- Header/Footer: Specifies a header and/or footer.
- Data Formats: Specifies how a bookmark displays, including style and content.
- Section Body Text: Specifies the layout and content of each section in the Body Text.
- Show Tab: Determines if this report or section displays in the View Report dropdown menu.
- Excluded: Provides the ability to exclude part of a report.

Configuring Section Body

Adding a section heading

→Highlight the Forensic Process row and right click. Select Edit from the context menu and choose the Body Text Tab. It should contain the code that lists the contents referenced by the bookmarks in the Forensic Process bookmark folder

```
list(path="Forensic Process")
```

→Insert the following text before this line. This text inserts a heading before the bookmark results in the style name Heading 1:

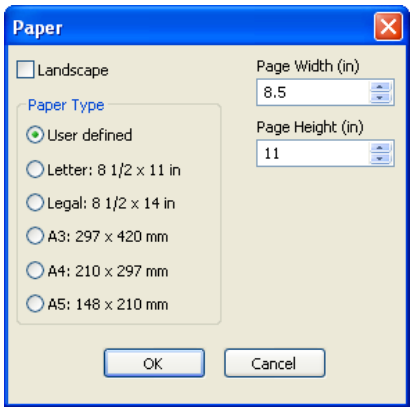
```
style("Heading 1") {text("Forensic Process")  par}
```

→ Repeat this process to add a heading to the Introduction Section

Configuring Paper Layout

Paper Size and Orientation

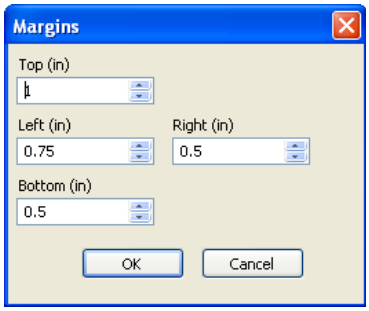
→ Highlight the Forensic Process row and right click the Paper column, and then click **Edit** in the dropdown menu. The Paper layout dialog opens.



→ Note paper size options including options for millimeters or inches, in addition **User defined** enables entries for any **Page Width** and **Page Height** boxes. The default orientation is Portrait. Note there is also an option to click the **Landscape** checkbox to change the orientation.

Margins

→ Right click the **Margins** column, and then click **Edit** in the dropdown menu. The Margins dialog opens.



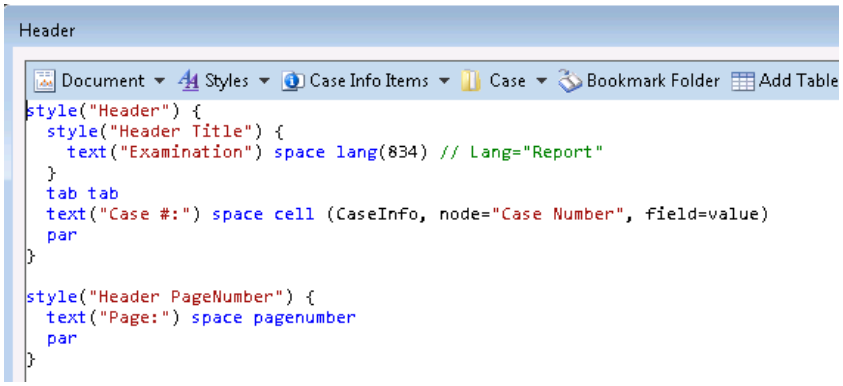
→ This dialog permits you to enter the margins you want in inches. By default, the top margin is 1 inch, the left margin is 0.75 inches, and the right and bottom margins are 0.5 inches.
→ Click Cancel.

Customizing Headers and Footers

You can customize the formatting of headers and footers and what information they contain.

→ Choose the Row for the Examination Report.
→ Right click the **Header** column, then click **Edit** in the dropdown menu.

→ Note the code in the header. This code defines default headers for the report. Do not change this code, but note that you can provide different headers and footers for the report and for different sections if you wish.



→ Note different formatting options (Document, Styles, Case Info Items, etc.) display at the top of the dialog.

→ Click Cancel.

Report Styles

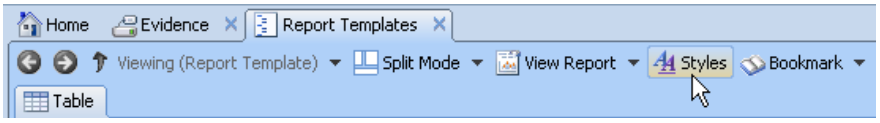
As in Microsoft Word, you use styles to set text formatting options. EnCase comes with many default styles to use in report templates, and you can also create your own styles. To override a default style, create a user style with the same name.

Style options include:

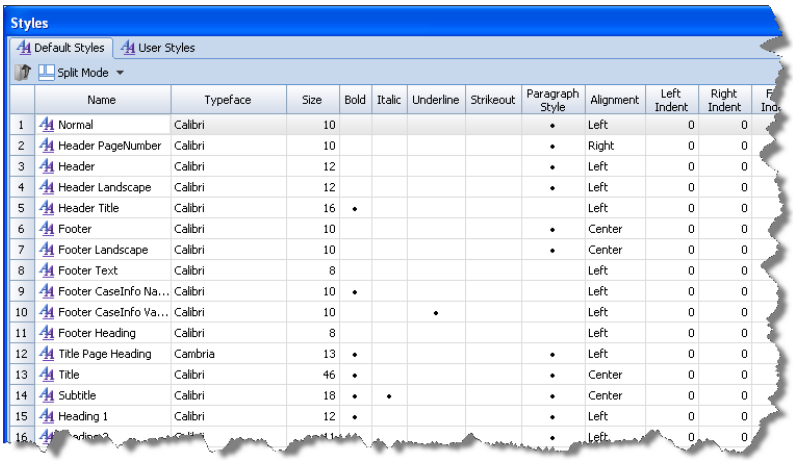
- Font type and size
- Alignment (centered, left and right justified)
- Indentation (left, right, first line)
- Space before/after
- Borders
- Tabs
- Text color
- Background color

To create a user defined style:

→ In the **Report Templates** tab, click **Styles** in the tab toolbar.



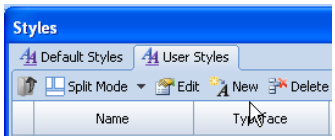
→ The Styles dialog opens, with tabs for **Default Styles** and **User Styles**.



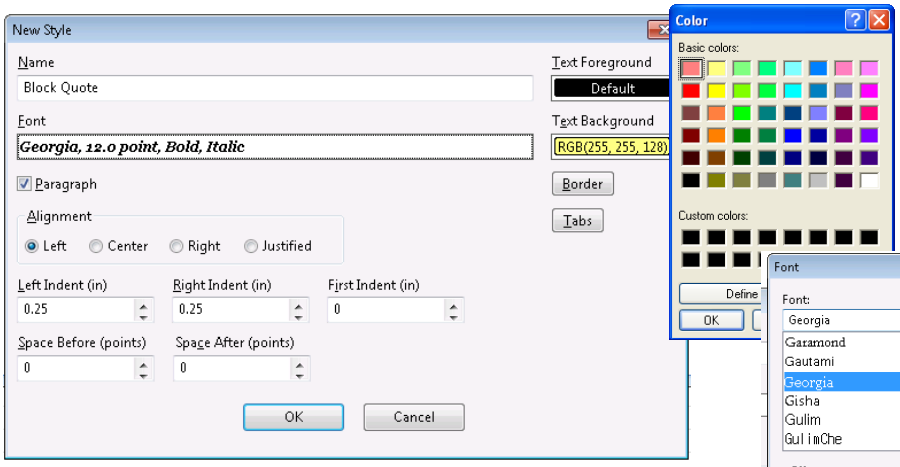
	Name	Typeface	Size	Bold	Italic	Underline	Strikeout	Paragraph Style	Alignment	Left Indent	Right Indent
1	Normal	Calibri	10					•	Left	0	0
2	Header PageNumber	Calibri	10					•	Right	0	0
3	Header	Calibri	12					•	Left	0	0
4	Header Landscape	Calibri	12					•	Left	0	0
5	Header Title	Calibri	16	•					Left	0	0
6	Footer	Calibri	10					•	Center	0	0
7	Footer Landscape	Calibri	10					•	Center	0	0
8	Footer Text	Calibri	8						Left	0	0
9	Footer CaseInfo Na...	Calibri	10	•					Left	0	0
10	Footer CaseInfo Va...	Calibri	10			•			Left	0	0
11	Footer Heading	Calibri	8						Left	0	0
12	Title Page Heading	Cambria	13	•				•	Left	0	0
13	Title	Calibri	46	•				•	Center	0	0
14	Subtitle	Calibri	18	•	•			•	Center	0	0
15	Heading 1	Calibri	12	•				•	Left	0	0
16	[illegible]	[illegible]	[illegible]					•	Left	0	0

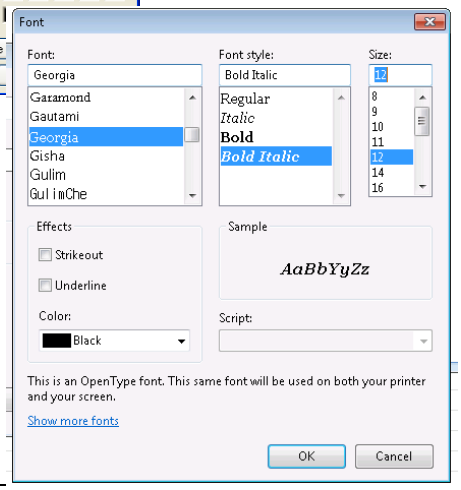
→ Select the **User Styles** tab.

→ Click **New** in the toolbar.



→ Create a new style by entering the name "Block Quote" for the style and your desired configuration options. Double click **Font**, **Text Foreground**, or **Text Background** to open dialogs for specifying text colors. Change the text background to yellow.





➔ Double click **Font** to open the Font dialog

- Change the Font face to Georgia
- Change style to Bold Italic

- Change the Size to 12 point
- Note Effects such as Strikeout, Underline and color

➔ Click OK

→ Click the **Paragraph** checkbox to set other options:

- Set Left Indent to 0.25 inches
- Set Right Indent to 0.25 inches
- Note other options: Alignment (Centered, Left and Right Justified) , First indent (in inches), Space Before (in points), Space After (in points)

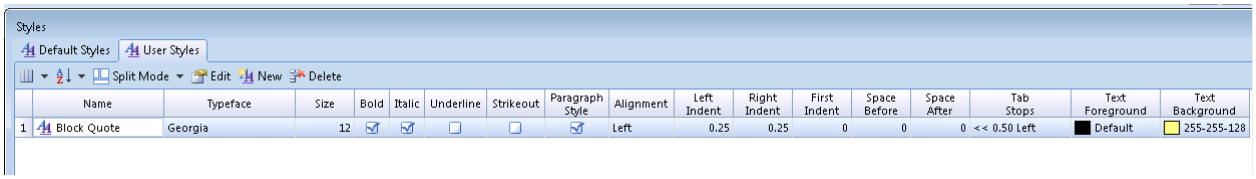
→ Click OK

→ Note the **Border** option. This enables you to set the position, size and color of any border lines you wish to incorporate.

→ To set tab stops within the style, click the **Tabs** button. Right click in the **Tabs** dialog and select **New** to create a new tab.

- In the **Alignment** box, choose **Left** (left side of the text block is aligned with the tab stop). Note others include **Center** (text is centered in relation to the tab) or **Right** (right side of the text block is aligned with the tab stop).
- Set the **Position** for the tab stop to 0.5 Inches.
- In the **Relative** box, choose **Left** to position the tab stop a set distance to the right of the left margin. Note others include **Center** to position it a distance from the center point between the margins, or **Right** to position it a set distance to the left of the right margin.

→ When you finish, click **OK**. The new style and its attributes display in the User Styles list.



You can also edit or delete an existing User Style.

Modifying Report Template Formats

EnCase now includes the ability to add additional metadata fields for entries and records to Report Templates. The report template builder makes all entry and record fields available and, if selected, the field values display in the report.

You can customize reports by specifying which fields to add to the report template. You can choose to include the value in the field as well as the name of the field. Then, when you generate a report, EnCase includes both specified fields and the content with which they are populated, in the specified area of the report.

All entry, record and item (bookmark) fields can be added to report templates. Multi-value fields, such as file extents and permissions, have two options for inclusion: cell and table. Adding the cell data displays the value of the field as displayed within the Entry table view. Adding the table data displays the value of the field as displayed in the Details tab.

Localization of Report Layout

Reports in EnCase are designed to work seamlessly in various regions regardless of local preferences such as paper size. If created properly, report templates print correctly on 8 ½" x 11" paper or A4 paper without requiring any changes to the templates.

All reports in EnCase obtain their paper settings from the Windows operating system. Windows stores paper size in the Default Printer settings, so unless a specific paper size is defined in a report template (**Paper** option), EnCase uses the paper size indicated there.

When reports are generated, margins are set for the indicated paper size and the report is rendered in that composition. Users should utilize the ability to set tab stops relative to a specific margin (described above) to ensure that tab stops also scale properly with the different paper variations. Report templates supplied with EnCase are configured in this manner.

Editing Report Object Code

In order to give users complete flexibility in how they format the data and look of a report, EnCase uses an optimized coding language called Report Object Code to specify the layout of pages and data. Report Object Code is used in the report body, header/footer, and in the formatting options for bookmarks. Report Object Code is similar to other scripting languages, but is specifically designed for this purpose. Guidance Software recommends that if you are interested in modifying a report template, or creating your own, to first refer to one of the supplied templates and see how Report Object Code is structured and used.

Example: Changing Template Contents

The report language can also be used to adjust which contents of each type of bookmark will be contained in the report, and the format can be selected. In this section we will modify Text types of bookmarks to include the comment field in the report.

→Select Report Templates Tab. Right click on the Documents Section. Choose Edit from the context menu.

→Select the Formats Tab. Right click on the Text File format and choose Edit from the context menu. The following code should appear in the editor.

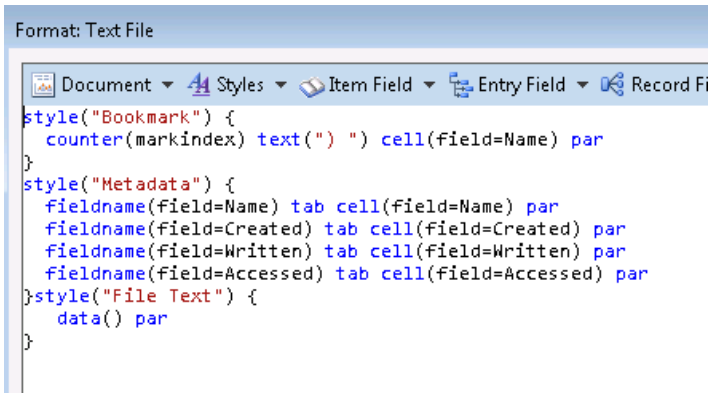


Figure 18. Text File Format.

→Move the cursor to the very beginning of the code. Choose "Styles" from the menu and choose "Block Quote". This should insert the following code in the editor:

```
style("Block Quote") {
     // text here
          par
           }
```

→ Select "// text here". Choose "Item Field" from the menu and choose "Comment". This should insert the following text in place of the selected text:

```
fieldname(field=Comment) tab cell(field=Comment)
```

→Verify the code window appears like the figure below. Choose "Compile" from the menu to reveal any errors. If none, choose Ok and OK.

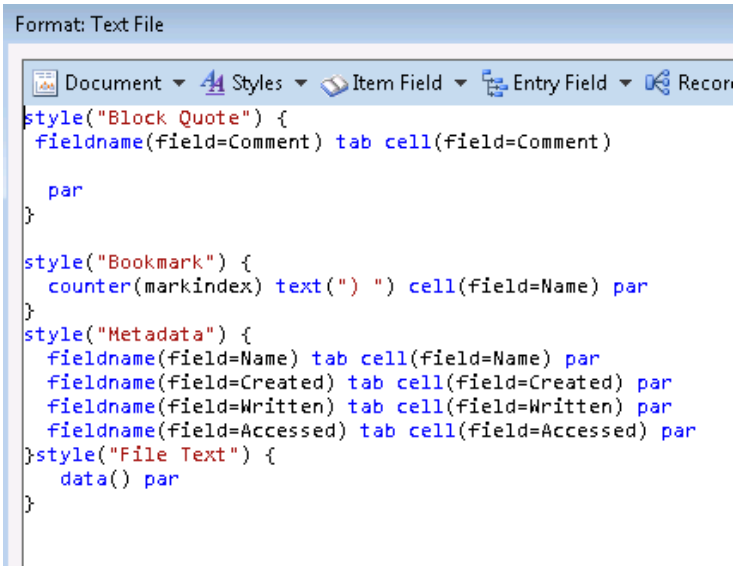


Figure 19. Modified Text File Format

→Check the report contents and verify that the Documents section now has Comments in the style created earlier.

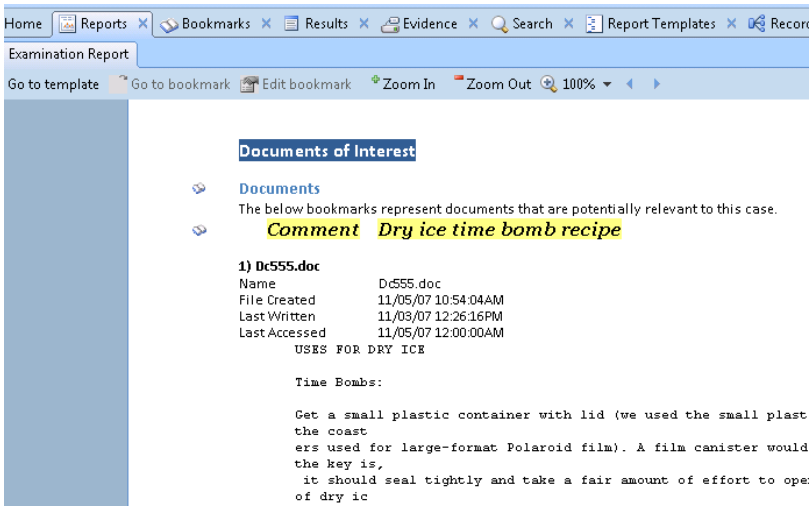


Figure 20. Bookmark Comments in Report.

Organizing Bookmarks Content

Our report contains all of the templates and bookmarked materials. Some of these were not important to include in the report. For example, there were no bookmarks in the Other Findings section.

→Select the <u>Report Templates Tab</u>, and select the Other Findings Section. Put a check in the "Excluded" box. View the report and verify that this section is no longer in the report.

→Select the <u>Bookmarks Tab</u> and create a new bookmark folder named "Notes and References"

→Select the Documents Folder and check item 4 in the Table pane. Click on the number "4" next to the check mark and drag it to the "Notes and References" Folder

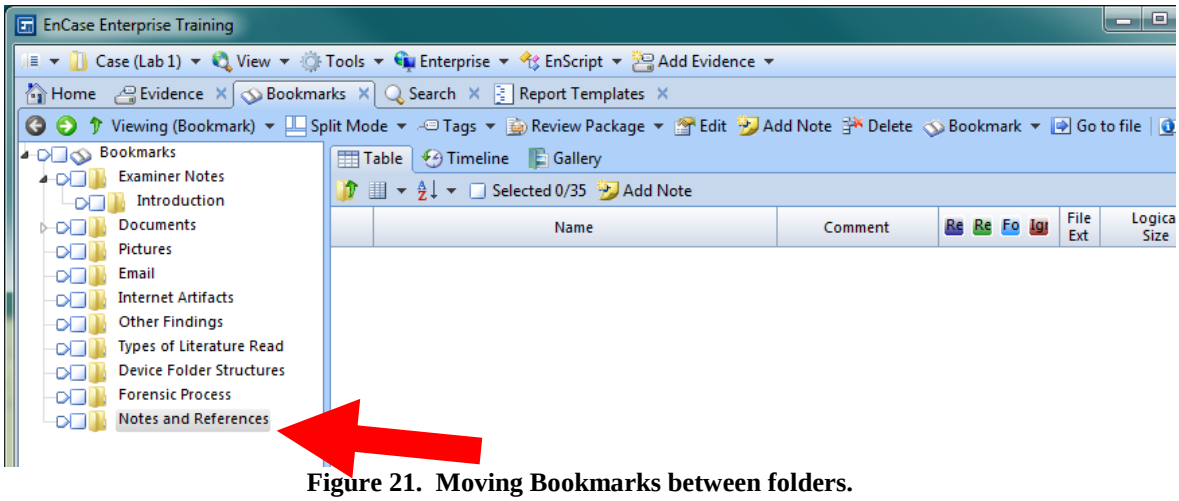


Figure 21. Moving Bookmarks between folders.

→Return to the Report Viewer and check the content of the report. The report should now be approximately 31 pages in length.

Saving the Report

→While viewing the report, right click anywhere in the report and choose "Save As". Choose RTF from the menu and note the location of the report. Change the file name to "Lab 1.rtf". Choose OK.

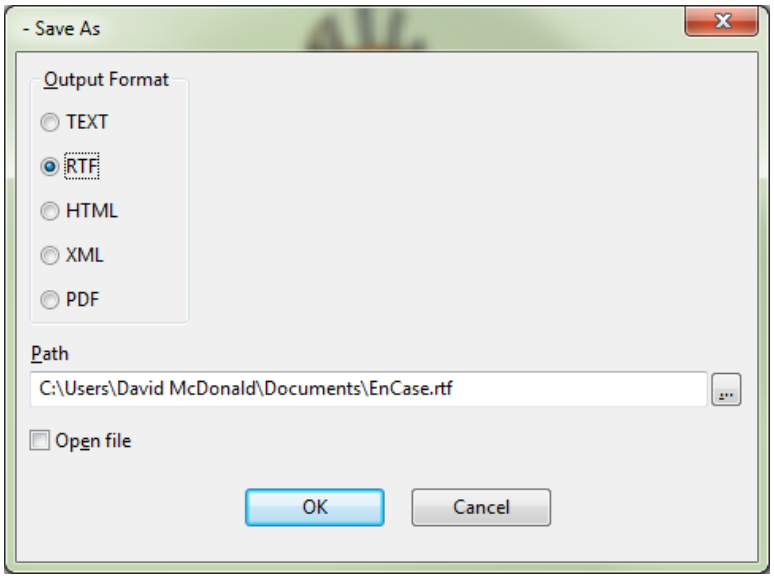


Figure 22. Saving the Report

→ The lab report can now be loaded into a word processing program, such as Microsoft Word, for further editing. Usually a professional report can be quickly completed with minor changes. For example, using Microsoft Word, the report

subheadings were automatically set to standard Word styles “Heading 1”, “Heading 2”, and “Heading 3”. The default style sheet created by Encase can be easily changed in Word.

→ Use SAVE AS on the .rtf report to create an MS Word .doc or .docx file using the naming convention:

*LastNameFirstNameInitial*Lab1.docx

→ Upload the report to the Lab1 DropBox in D2L.

Note: Many forensics examiners will produce both a printed report and a supplementary CD. For example, our “Notes and references” material could be produced as a separate HTML file. The HTML export provides an initial framework for an electronic supplement to a printed forensics report.