CEIC® 2014

Examination Reporting Made Easy

Ken Mizota
Sr. Product Manager, Guidance Software

www.encase.com/ceic

Agenda

- What is an Examination Report?
- What You Need To Know: Reporting Concepts
- Hands-on: Your First Report
- EnCase 7.10 Preview of Reporting
- Questions

Examination Reporting Made Easy CEIC 2014

What is an Examination Report?

Your have performed a thorough investigation and you're ready to wrap it up.

Your Examination Report should be:

- Well-organized
- Presented in a format the target audience will understand

Page 3

Examination Reporting Made Easy CEIC 2014

What is an Examination Report?

Reporting is a chore.

The findings of each case are unique, but commonalities across cases exist.

- Styles and Formatting of findings
- Images or Logos
- Disclaimers, Legalese
- Similar bookmark structures for similar types of cases

You shouldn't need to perform this work for EVERY case.

Page 4

Examination Reporting Made Easy — CEIC 2014

What is an Examination Report?

EnCase makes examination reporting easy by:

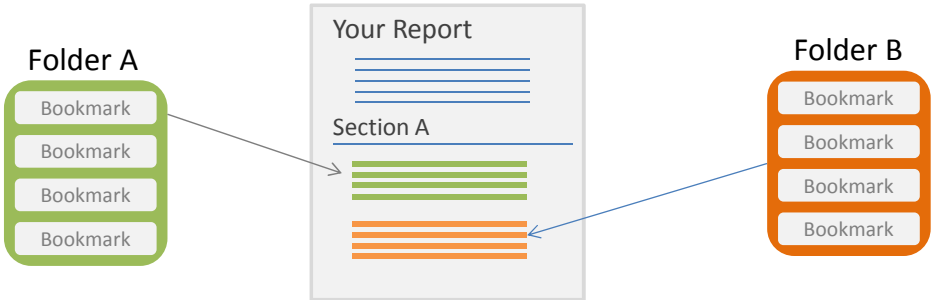
- Powerful, automated reporting of bookmarks/findings
- Simplified organization of reporting elements
- Reduced time spent by template re-use

Page 5

Examination Reporting Made Easy — CEIC 2014

Concepts: Bookmarks

- Bookmarks and Bookmark Folders are the content for your report
- Each Bookmark Type can have a unique Bookmark Format for display
- The following slides depict a few samples of Report output for specific Bookmark Types

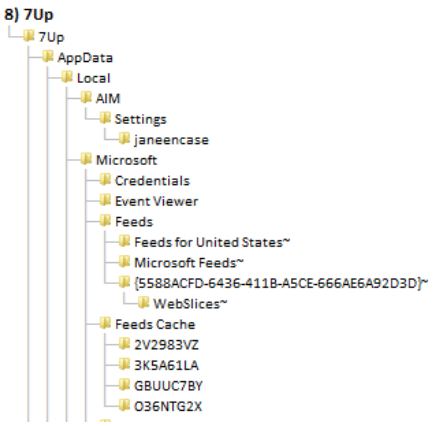


Page 6

Examination Reporting Made Easy CEIC 2014

Bookmark Type Format Samples

Tree/Folder Bookmark

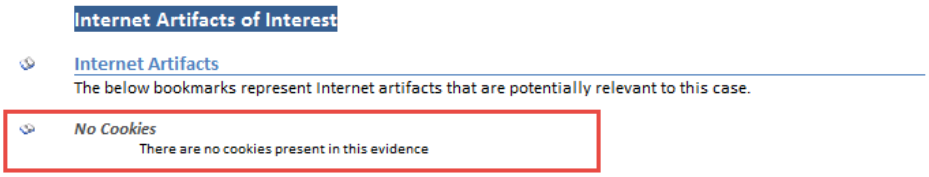


Page 7

Examination Reporting Made Easy CEIC 2014

Bookmark Type Format Samples

Note Bookmark



Page 8

Examination Reporting Made Easy CEIC 2014

Bookmark Type Format Samples

Text File = Highlighted Text

9) conf-chat1291066436515.html

Item Path	v7_Sample_Evidence\C\Users\7Up\Documents\AIMLogger\janeencase\IM Logs\conf-chat1291066436515.html
File Created	04/26/11 08:07:03 AM
Last Written	11/29/10 01:06:04 PM
Last Accessed	04/26/11 08:07:03 AM
MD5	
Comment	Indication of motive

"I don't think she's going to pass inspection"

Page 9

Examination Reporting Made Easy CEIC 2014

Bookmark Type Format Samples

Data bookmark = Table

1) Table View of an Entry

Item Path Table View of an Entry

Comment

	Name	File Ext	Logical Size	Signature Analysis	File Type
1	v7_Sample_Evidence		0		
2	C		4,096		
3	Users		136		
4	7Up		4,096		
5	Documents		4,096		
6	AIMLogger		472		
7	janeencase		248		
8	IM Logs		4,096		
9	conf-chat1291066436515.html	html	5,436		

Page 10

Examination Reporting Made Easy — CEIC 2014

Bookmark Type Format Samples

Image

2) 4CABF05767DC4331286A9438B4BD9[1].jpg

Item Path	v7_Sample_Evidence\C\Users\7Up\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\9UH3UQRX\4CABF05767DC4331286A9438B4BD9[1].jpg
File Created	12/14/10 02:15:33 PM
Last Written	12/14/10 02:15:33 PM
Last Accessed	12/14/10 02:15:33 PM
MD5	374cabf05767dc43031286a9438b4bd9
Comment	

Examination Reporting Made Easy — CEIC 2014

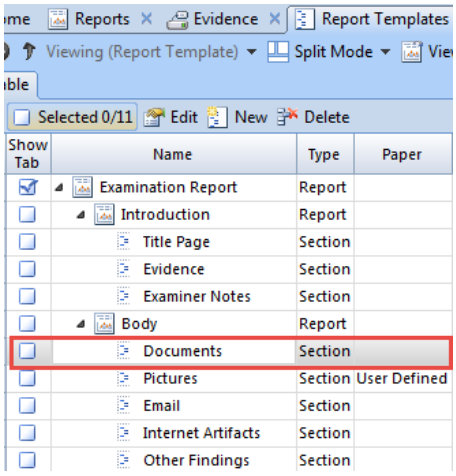
Concepts: Report Templates

- A Report Template controls:
  - the display of Bookmark Folders
    - *"Is this Bookmark Folder in the report?"*
  - the order of display Bookmark Folders
    - *"Should bookmarks on Brutus appear before Suspect B's?"*
  - the format and style of Bookmarks
    - *"How should Bookmarks for Brutus and Popeye be presented?"*
  - Page Formatting
    - e.g. Headers, footers, titles, page numbers

Examination Reporting Made Easy CEIC 2014

Concepts: Report Templates

- A Report Template consists of Sections
- Each Section consists of:
  - Body Text
    - *"What Bookmarks will be displayed in this Report Section?"*
  - Bookmark Formats
    - *"How will Bookmarks be displayed in this Report Section?"*
  - Page Formatting
    - *"Should this section be Landscape or Portrait orientation?"*



Examination Reporting Made Easy CEIC 2014

Your First Report

- Goal: Create Bookmarks and View your Report
- Duration: 10 mins
- Create a New Case
  - Case Name: MyCase
  - Evidence Cache: <Examination Reporting The Easy Way>
  - Use Template: #1 Basic

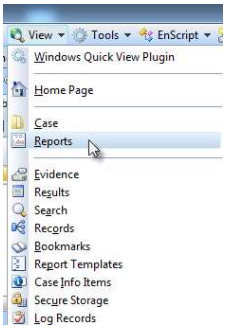
Examination Reporting Made Easy

CEIC 2014

Your First Report

- Find evidence, and create Bookmarks and place in specific folders:
  - Create a new Bookmark Folder “Suspect → Brutus”
  - Internet Artifact Record → “Suspect → Brutus” Bookmark Folder

View the Report!



Page 15

Examination Reporting Made Easy

CEIC 2014

Your First Report

- You’re in good shape if you have:
  - The metadata you needed to describe your Bookmarks
  - Bookmark Folders are in your Report Template

… but what if metadata you need is not in the report?

… what if your Bookmark Folders don’t appear in the report?

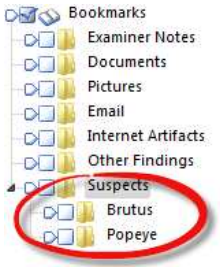
… what if you want your logo on the title page?

Page 16

Examination Reporting Made Easy — CEIC 2014

Customizing Metadata

- A Report Template controls:
  - the display of Bookmark Folders
    - *"Is this Bookmark Folder in the report?"*
  - the order of display Bookmark Folders
    - *"Should bookmarks on Brutus appear before Suspect B's?"*
  - the format and style of Bookmarks
    - *"How should Bookmarks for Brutus and Popeye be presented?"*
  - Page Formatting
    - e.g. Headers, footers, titles, page numbers

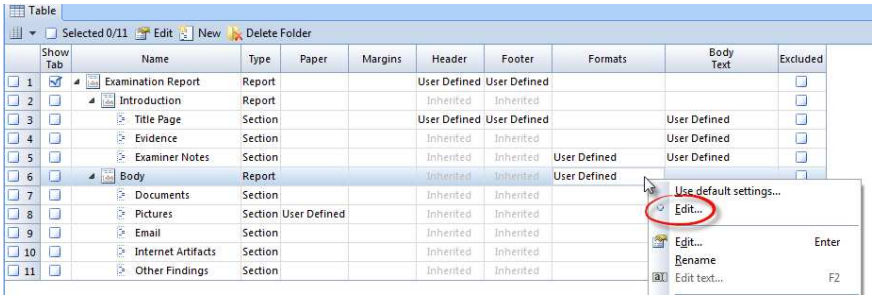


Page 17

Examination Reporting Made Easy — CEIC 2014

Your First Report

- Customizing Metadata
  - Edit the Format that applies to the section you are working with.
  - Formats may be set at the Section level and can be inherited to child Sections



	Show Tab	Name	Type	Paper	Margins	Header	Footer	Formats	Body Text	Excluded
1	☑	Examination Report	Report			User Defined	User Defined			
2	☐	Introduction	Report			Inherited	Inherited			
3	☐	Title Page	Section			User Defined	User Defined		User Defined	
4	☐	Evidence	Section			Inherited	Inherited		User Defined	
5	☐	Examiner Notes	Section			Inherited	Inherited	User Defined	User Defined	
6	☐	Body	Report			Inherited	Inherited	User Defined		
7	☐	Documents	Section			Inherited	Inherited			
8	☐	Pictures	Section	User Defined		Inherited	Inherited			
9	☐	Email	Section			Inherited	Inherited			
10	☐	Internet Artifacts	Section			Inherited	Inherited			
11	☐	Other Findings	Section			Inherited	Inherited			

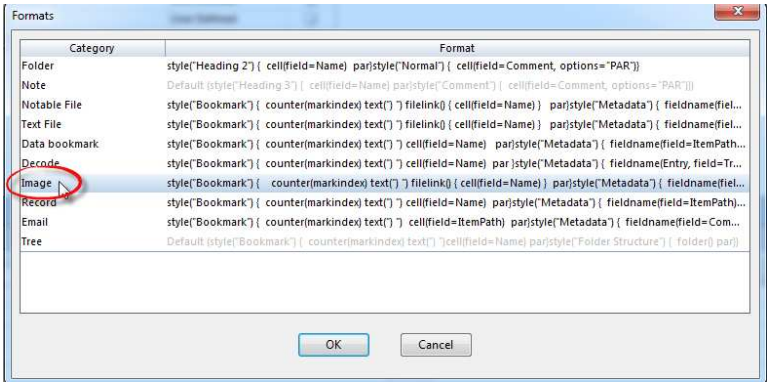
Page 18

Examination Reporting Made Easy

CEIC 2014

Your First Report

- Customizing Metadata
  - Double-click Image



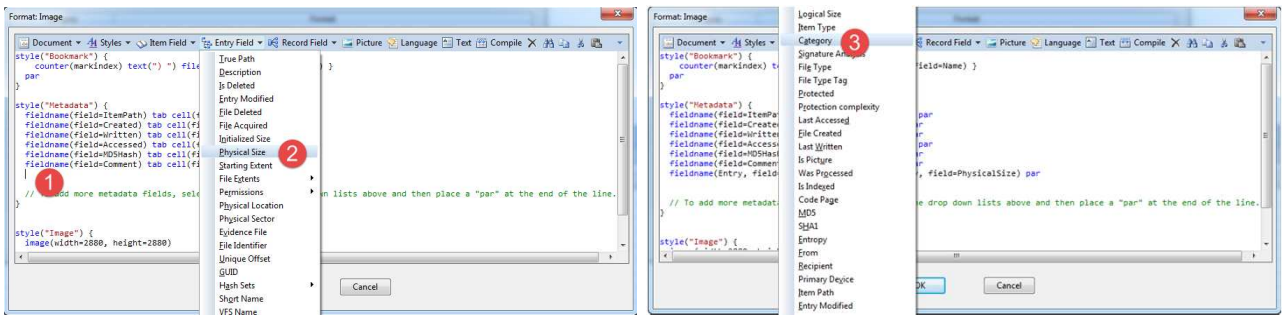
Page 19

Examination Reporting Made Easy

CEIC 2014

Your First Report

- Customizing Metadata
  - Add “Physical Size” and “Category”



Page 20

Examination Reporting Made Easy CEIC 2014

Your First Report

- Customizing Metadata

2) 4CABF05767DC4331286A9438B4BD9[1].jpg

Item Path	v7_Sample_Evidence\C\Users\7Up\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\9UH3UQRX\4CABF05767DC4331286A9438B4BD9[1].jpg
File Created	12/14/10 02:15:33 PM
Last Written	12/14/10 02:15:33 PM
Last Accessed	12/14/10 02:15:33 PM
MD5	374cabf05767dc43031286a9438b4bd9
Comment	
Physical Size	16,384
Category	Picture

Examination Reporting Made Easy CEIC 2014

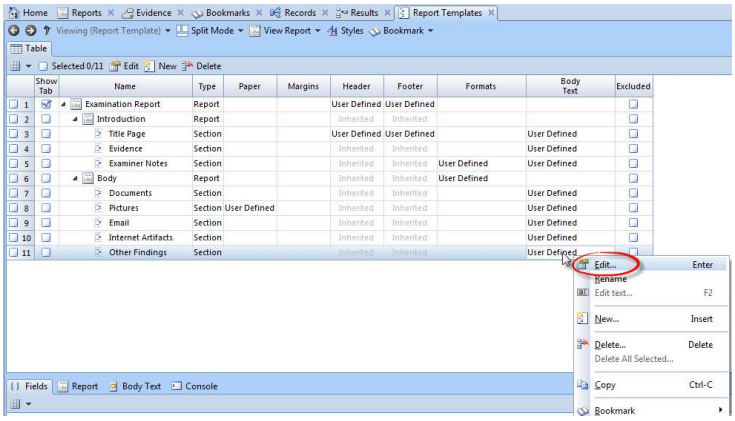
Adding a Bookmark Folder to Your Report

- A Report Template controls:
  - the display of Bookmark Folders
    - *"Is this Bookmark Folder in the report?"*
  - the order of display Bookmark Folders
    - *"Should bookmarks on Brutus appear before Suspect B's?"*
  - the format and style of Bookmarks
    - *"How should Bookmarks for Brutus and Popeye be presented?"*
  - Page Formatting
    - e.g. Headers, footers, titles, page numbers

Examination Reporting Made Easy CEIC 2014

Your First Report

- Adding a Bookmark Folder to your Report
- Edit → Body Text

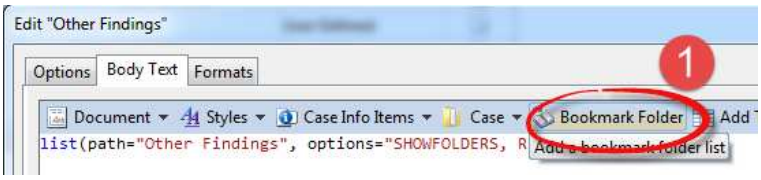


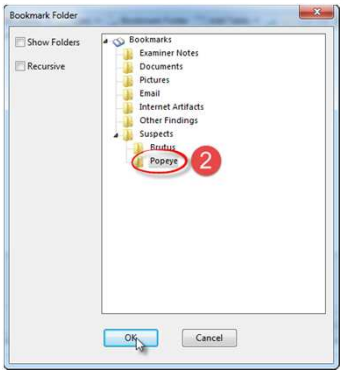
Page 23

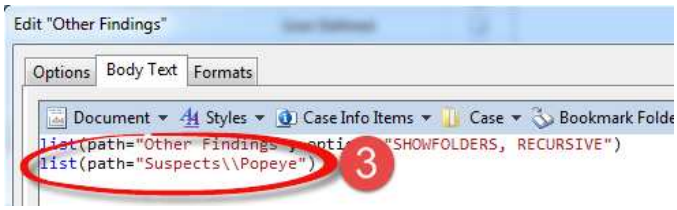
Examination Reporting Made Easy CEIC 2014

Your First Report

- Adding a Bookmark Folder to Your Report



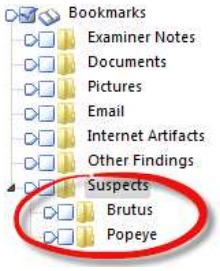




Page 24

Examination Reporting Made Easy — CEIC 2014

Changing the Title Page Logo

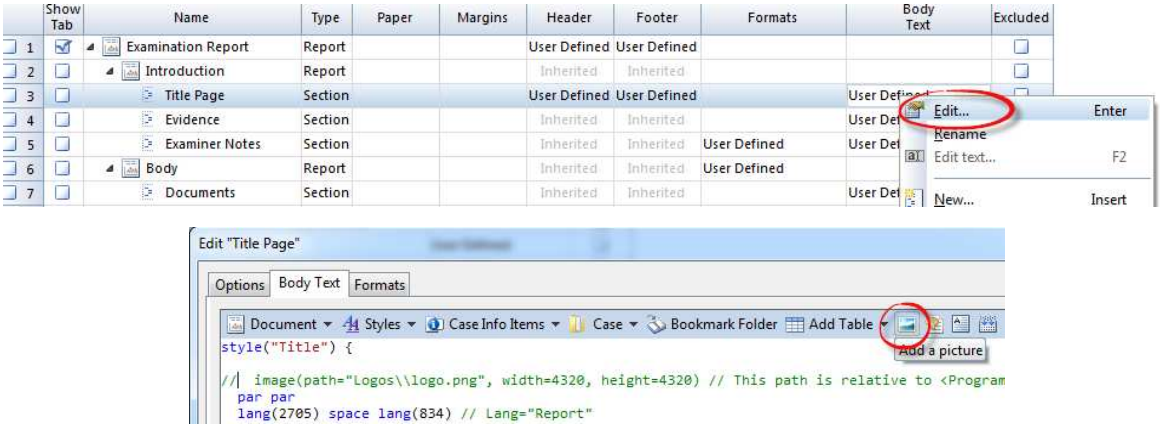


- A Report Template controls:
  - the display of Bookmark Folders
    - *"Is this Bookmark Folder in the report?"*
  - the order of display Bookmark Folders
    - *"Should bookmarks on Brutus appear before Suspect B's?"*
  - the format and style of Bookmarks
    - *"How should Bookmarks for Brutus and Popeye be presented?"*
  - Page Formatting
    - e.g. Headers, footers, titles, page numbers

Examination Reporting Made Easy — CEIC 2014

Your First Report

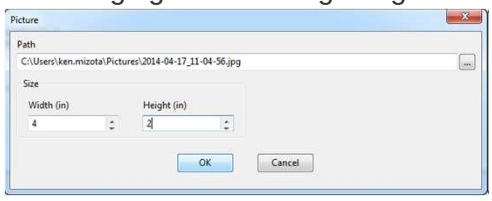
- Changing the Title Page Logo

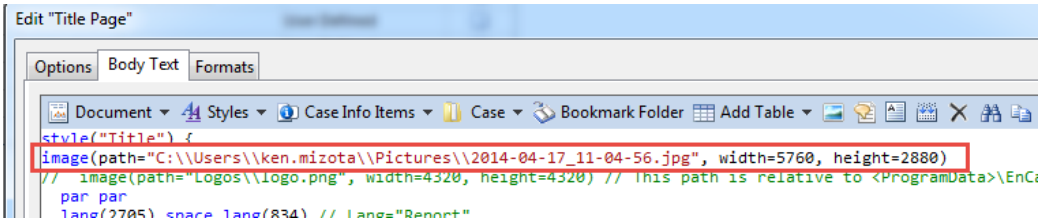


Examination Reporting Made Easy CEIC 2014

Your First Report

- Changing the Title Page Logo



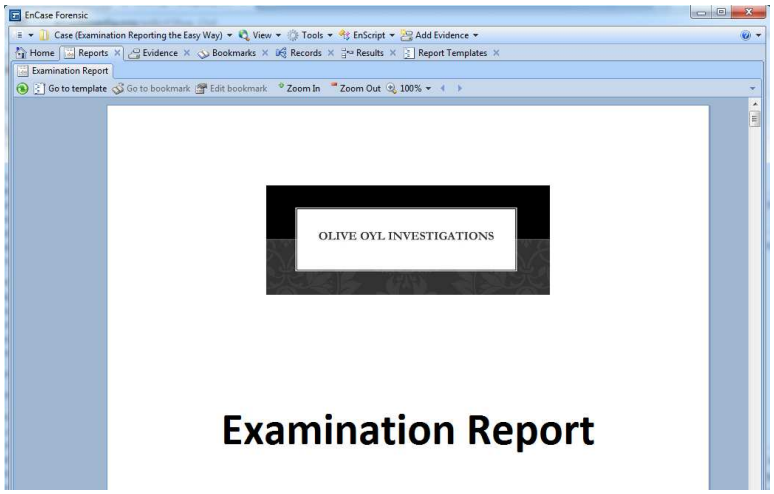


Page 27

Examination Reporting Made Easy CEIC 2014

Your First Report

- Changing the Title Page Logo

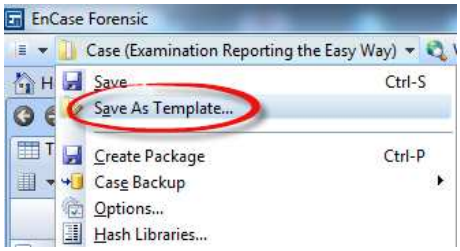


Page 28

Examination Reporting Made Easy CEIC 2014

Re-use, Recycle

- Save your case as a template, so you may make use of your work in subsequent investigations.
- Bookmark Folders and Report Templates will be maintained for future use



Page 29

Examination Reporting Made Easy CEIC 2014

EnCase 7.10 Preview: Formatting Wizard

- Makes common tasks much easier
  - Specify and order metadata
  - Assign Bookmark Folder to a Report Section
  - Hide pictures

Coming in July 2014

Page 30

Examination Reporting Made Easy CEIC 2014

Questions?

Page 31