BIRMINGHAM CITY
University

Forensic Investigation Reporting

Dr Syed Naqvi

syed.naqvi@bcu.ac.uk

The Higher Education Academy

Outline

- Definitions
- Investigation reports
- Personal testimony
- Equipment handling

Some basics …

- Forensics investigation report
  - Provides statement of findings
- Expert report
  - Provides an opinion
- Expert witness
  - Provides insight that common sense does not offer
    - Conclusions are drawn

Guidelines

- Fraud Examiners Manual
- Important considerations are:
  - Organization and work flow
  - Accuracy
  - Clarity
  - Impartiality
  - Relevance
  - Timeliness

Prescriptive Statements

- Introductory material
- Organisation and style
- Data reporting
- Interpretations and opinion

Investigation report

- Used for legal proceedings and for incidence response.
- Findings:
  - Why was the evidence reviewed?
  - How was the evidence reviewed?
  - How did the forensic examiner arrive at conclusions?
- Conclusions are:
  - Clearly explained.
  - Supported.
  - Possibly lead to recommendations.

Investigation report – thumb rules

- Accurately describe the details of an incident.
- Be understandable to decision makers.
- Be able to withstand legal scrutiny.
- Be unambiguous and not open to misinterpretation.
- Be easily referenced (Bates numbering)
- Contains all information required to explain the conclusions
- Offer valid conclusions, opinions, or recommendations when needed.
- Be created in a timely manner.

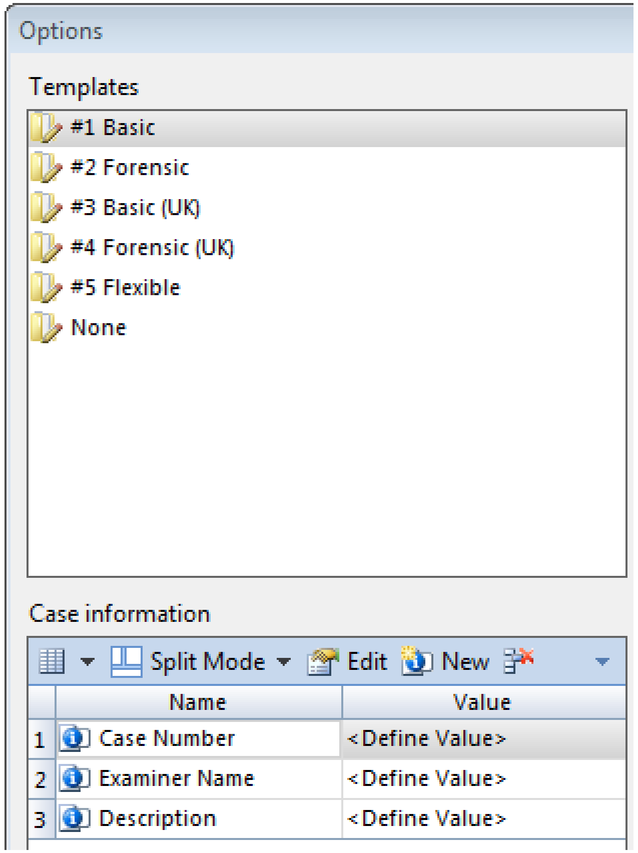
Investigation report – Organisation

- Macro to Micro
- Template
- Formatting:
  - Consistent identifiers
  - Attachments and Appendices
  - **Proofread by others**

Investigation report – Contents

- Computer Evidence Analysed
  - Detailed description of evidence
  - Linked with bookmarks.
- Relevant Findings
- Supporting Details
- Investigative Leads
- Additional Report Sections

EnCase – Report Generator



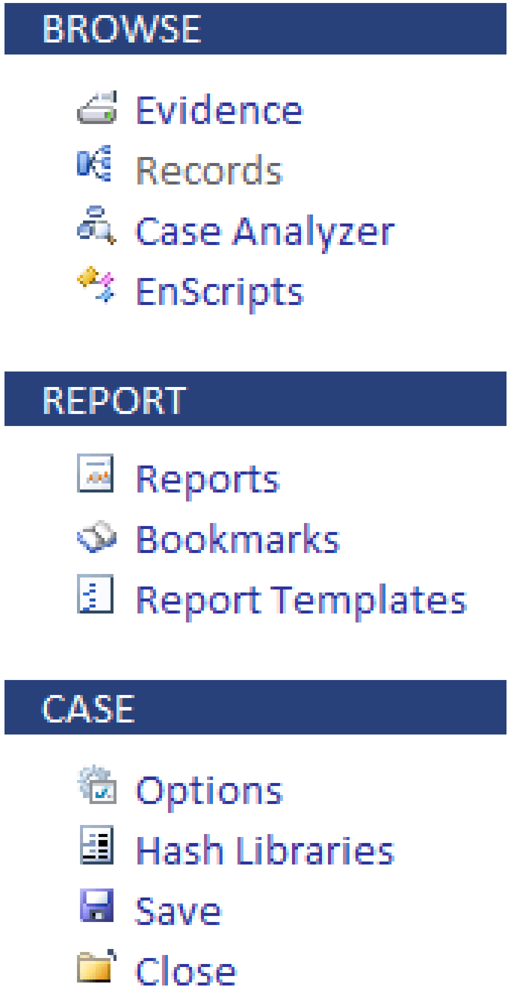
Options

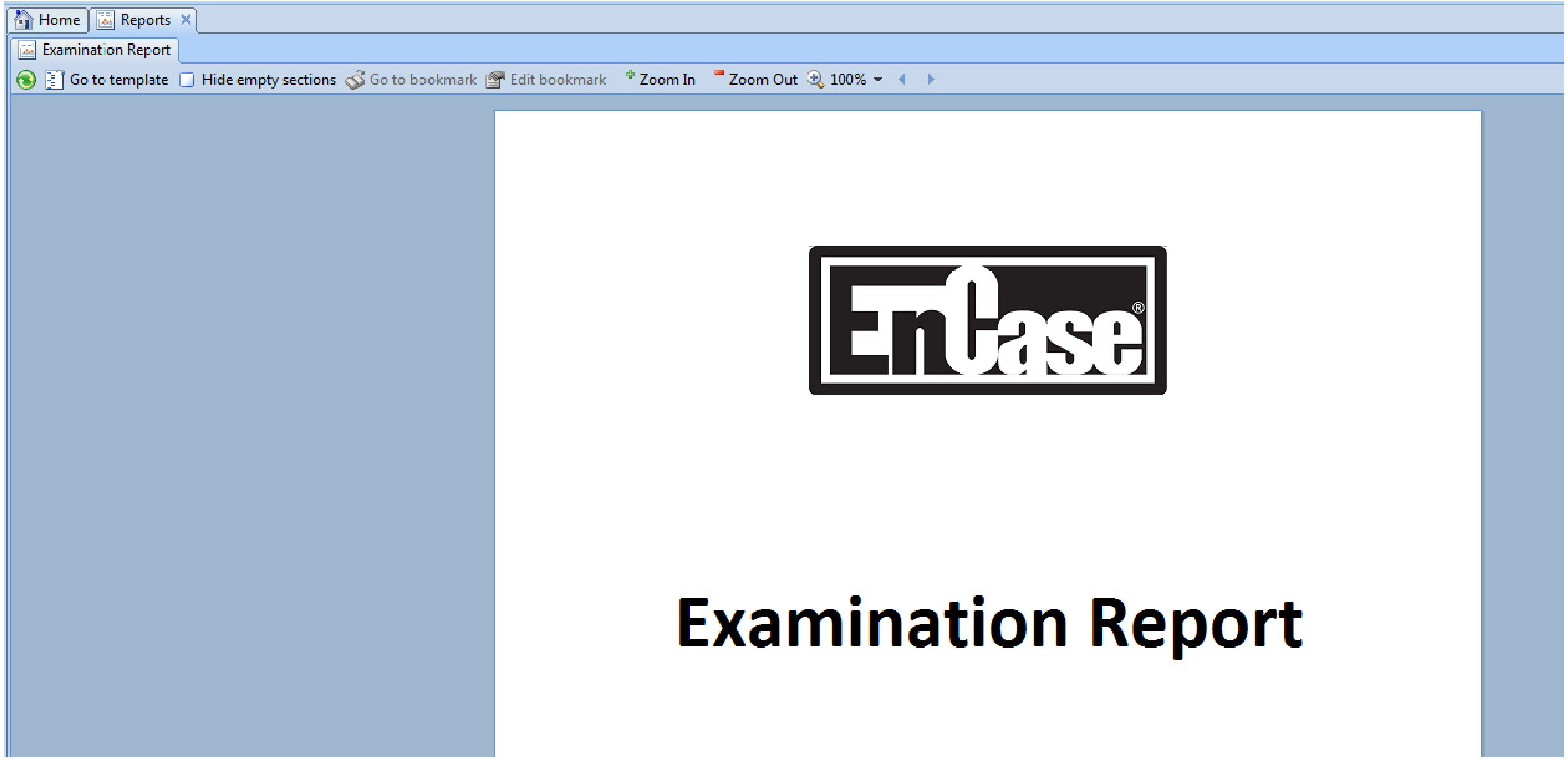
Templates

- #1 Basic
- #2 Forensic
- #3 Basic (UK)
- #4 Forensic (UK)
- #5 Flexible
- None

Case information

	Name	Value
1	Case Number	<Define Value>
2	Examiner Name	<Define Value>
3	Description	<Define Value>

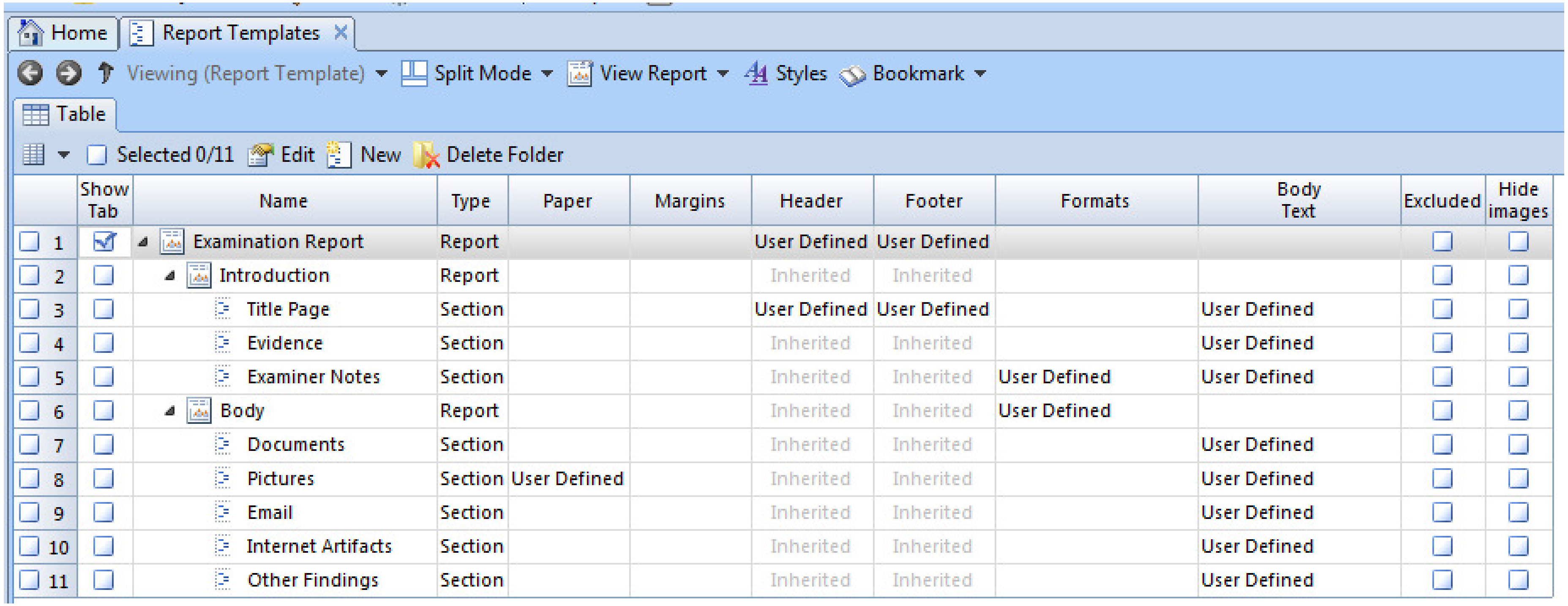




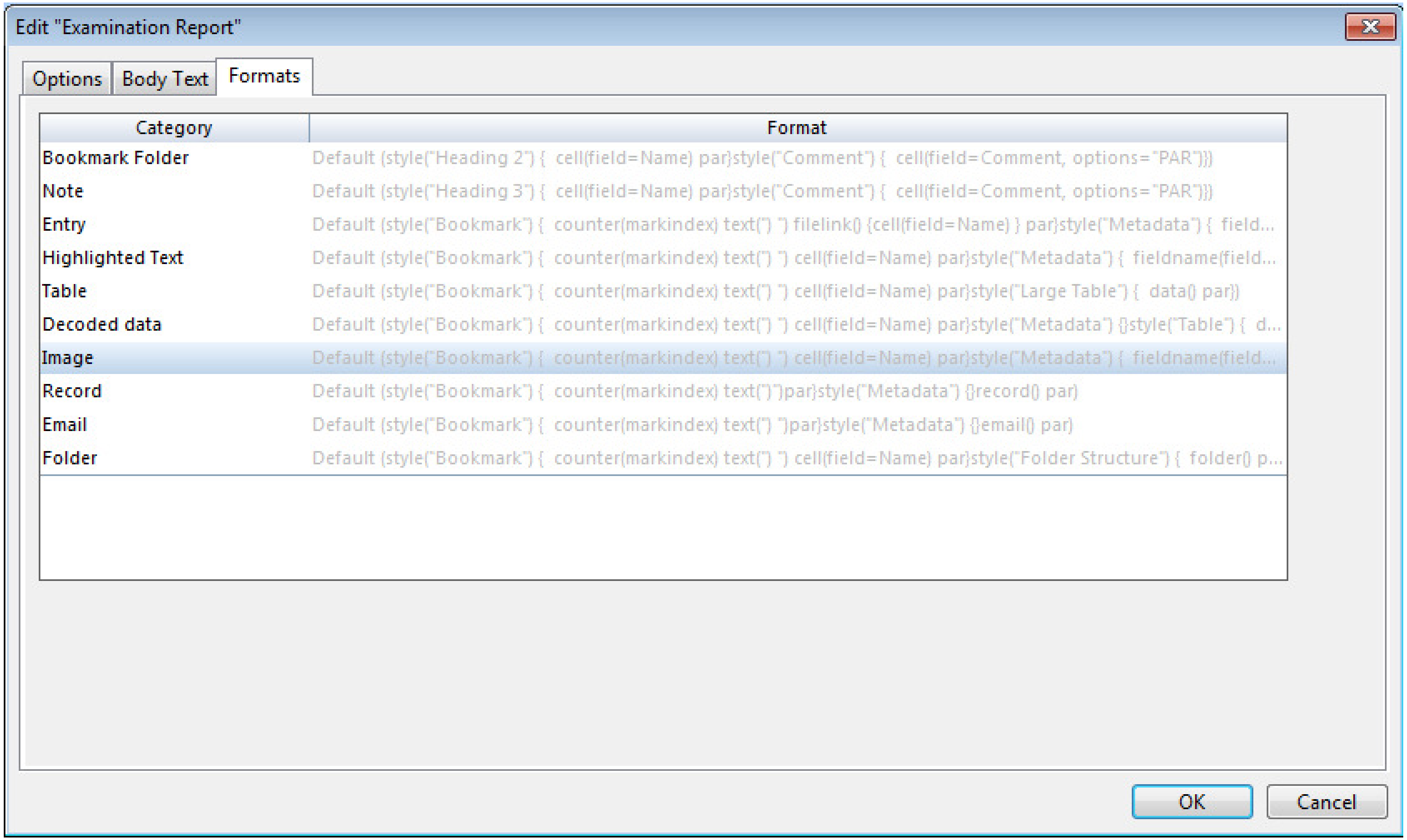
Examination Report

Change the logo …

- Replace EnCase logo with the BCU logo



		Show Tab	Name	Type	Paper	Margins	Header	Footer	Formats	Body Text	Excluded	Hide images
□	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		User Defined	□	□
□	8	□	Pictures	Section	User Defined		Inherited	Inherited		User Defined	□	□
□	9	□	Email	Section			Inherited	Inherited		User Defined	□	□
□	10	□	Internet Artifacts	Section			Inherited	Inherited		User Defined	□	□
□	11	□	Other Findings	Section			Inherited	Inherited		User Defined	□	□



Category	Format
Bookmark Folder	Default (style("Heading 2") { cell(field=Name) par}style("Comment") { cell(field=Comment, options="PAR")})
Note	Default (style("Heading 3") { cell(field=Name) par}style("Comment") { cell(field=Comment, options="PAR")})
Entry	Default (style("Bookmark") { counter(markindex) text(") ") filelink() {cell(field=Name) } par}style("Metadata") { field...
Highlighted Text	Default (style("Bookmark") { counter(markindex) text(") ") cell(field=Name) par}style("Metadata") { fieldname(field...
Table	Default (style("Bookmark") { counter(markindex) text(") ") cell(field=Name) par}style("Large Table") { data() par})
Decoded data	Default (style("Bookmark") { counter(markindex) text(") ") cell(field=Name) par}style("Metadata") {}style("Table") { d...
Image	Default (style("Bookmark") { counter(markindex) text(") ") cell(field=Name) par}style("Metadata") { fieldname(field...
Record	Default (style("Bookmark") { counter(markindex) text(")")par}style("Metadata") {}record() par)
Email	Default (style("Bookmark") { counter(markindex) text(") ")par}style("Metadata") {}email() par)
Folder	Default (style("Bookmark") { counter(markindex) text(") ") cell(field=Name) par}style("Folder Structure") { folder() p...