- Explain the rules for digital evidence
- Describe how to collect evidence at private-sector incident scenes
- Explain guidelines for processing law enforcement crime scenes
- List the steps in preparing for an evidence search
- Describe how to secure a computer incident or crime scene
- Explain guidelines for seizing digital evidence at the scene
- List procedures for storing digital evidence
- Explain how to obtain a digital hash
- Review a case to identify requirements and plan your investigation

Outcome 4:

Investigate Digital Forensic tools and their use for Forensic Analysis and Validation

- Determine what data to analyse in a computer forensics investigation
- Explain common data-hiding techniques
- Analyse tools used to acquire and validate data including Network, Cell Phone and Mobile Device Forensics Tools
- Describe methods of performing a remote acquisition
- Explain standard procedures for performing a live acquisition and network forensics

Outcome 5:

Select suitable analysis tools and apply them in a simulated investigation

- Prepare and plan a forensic investigation based on an authentic situation
- Perform and document the investigation described in the plan

Assessment:

Weighting	**Nature of assessment**	**Learning outcomes**
20%	Test(s)	1,2,3
40%	Written report that includes the analysis of tools, investigation plan and findings from case study scenarios	4,5
40%	Final Exam	1,2,3,4

Learning and teaching approaches: Lectures, Laboratory work, Self- directed study.

Learning resources required:

Textbook: Refer to the current programme booklist.

Learning resources recommended: