Learning outcomes:

	Learning outcomes
1.	Discuss Computer Investigation
2.	Explain Data Sources and Acquisition Methods
3.	Describe how to secure a Computer Incidence or Crime Scene
4.	Investigate Digital Forensic tools and their use for Forensic Analysis and Validation
5.	Select suitable analysis tools and apply them in a simulated investigation

Topics/Content outline:

- Understanding Computer Investigations
- The Investigator's Office and Laboratory
- Data Acquisition
- Processing Crime and Incident Scenes
- Current Computer Forensics Tools
- Computer Forensics Analysis and Validation
- Recovering Graphics Files
- Network Forensics
- E-mail Investigations
- Cell Phone and Mobile Device Forensics
- Report Writing for High-Tech Investigations

Expanded Outcomes
Outcome 1: **Discuss Computer Forensic Investigation** • Explain how to prepare a computer forensic investigation • Apply a systematic approach to an investigation • Describe procedures for corporate high-tech investigations • Explain requirements for data recovery workstations and software • Describe how to conduct an investigation and the ethical considerations • Explain how to complete and critique a case
Outcome 2: **Explain Data Sources and Acquisition Methods** • List digital evidence storage formats • Explain ways to determine the best acquisition method • Describe contingency planning for data acquisitions • Explain how to use acquisition tools • Explain how to validate data acquisitions • Describe RAID acquisition methods • Explain how to use remote network acquisition tools • List other forensic tools available for data acquisitions
Outcome 3: **Describe how to secure a Computer Incidence or Crime Scene**