

Introduction to Investigations using Digital Forensics, Electronic Disclosure / eDiscovery



Discovery refers to discovery in legal proceedings such as litigation, government investigations, or Freedom of Information Act requests and regulatory investigations where the information sought is in electronic format (often referred to as electronically stored information or ESI). There is need for understanding for how to store digital data and how to retrieve it when required/requested. The course will provide professionals with a high-level understanding of what can be done during an investigation and when to reach out to experts.

Course Component (inc. hours)		Takeaways	Learning Objectives
Unit 1: A brief overview of digital forensics & electronic disclosure/discovery	25 mins	<ul style="list-style-type: none">• Recognise the importance and role of data and technology in investigations• Understand how to approach the use of digital data• Understand the scale of digital data and how digital forensics is used to preserve, investigate, and interpret it.	By exploring the core fundamentals of the topic, begin to appreciate how their effective management contributes to better outcomes in investigations.
Unit 2 – Digital Forensics	20 mins	<ul style="list-style-type: none">• Explain best practice in data collection• Identify the different types of metadata• Recognise some of the pitfalls in data preservation	Build on your core understanding to consider the role of digital forensics in the preservation, investigation, and interpretation of data. Start to explore what's possible when using digital forensic techniques and methodologies.
Unit 3 – Digital Forensics in Practice	40 mins	<ul style="list-style-type: none">• Explain the practical techniques used in digital forensics• Understand how to spot inconsistencies in data• Detect when data has been deleted and what to do to recover it.	Use interactive graphics to explore practical techniques used within digital forensics to improve investigations. Some of the common user actions that you may encounter in investigations are explained, with examples of how to unpick these.

Course Component (inc. hours)		Takeaways	Learning Objectives
Unit 4 – Introduction to Electronic Disclosure/ Discovery	30 mins	<ul style="list-style-type: none"> • Explain the role of eDiscovery technology and identify where and how it can assist in investigations • Recognise common eDiscovery techniques and how technology supports them • Understand techniques for managing large volumes of data effectively. 	Follow a typical journey that data takes when using eDiscovery technology and explore how large volumes of data can be managed to improve your investigation efficiency.
Unit 5 – Further techniques in electronic disclosure/ discovery	40 mins	<ul style="list-style-type: none"> • Understand why email threading is useful and how it can help you pinpoint missed conversations • Explain the significance of even small differences in files and the importance of deduplication • Recognise different techniques to help visualise data and present it in a meaningful way 	<p>Take your learning a stage further by exploring some of the more advanced analysis and methods of eDiscovery technology which can be used in investigation scenario, covering:</p> <ol style="list-style-type: none"> 1. Email threading 2. Near duplicates and associated methods 3. Predictive coding and continuous active learning, and 4. Data visualisation.