Put your digital investigative skills to the test with Operation Modify

Published on 6 April 2023

Our interactive resource helps you develop your understanding of digital opportunities for intelligence and investigation – one episode at a time

News   6 mins read

Operation Modify (also known as Op Modify) helps new and serving officers, police staff and volunteers to acquire the digital skills they need to undertake investigations effectively.

Op Modify consists of 15 episodes on College Learn (you will need to log in). These include:

- 10 episodes in the boxset, 'Improving digital thinking'
- four episodes in the sequel, 'Developing digital thinking'
- a 'Digital spotlight on violence against women and girls (VAWG)' module

Each episode follows the events from the beginning of an initial incident to show how to identify sources of digital evidence and respond to digital opportunities.

Completing Op Modify counts towards your personal continuing professional development (CPD). The series' learning outcomes map directly onto the digital elements of the **policing education qualifications framework (PEQF)** and can be used as supporting material for:

- the **police constable degree apprenticeship (PCDA)**
- the Professionalising Investigations Programme level 1 (PIP 1)
- **Fast Track entry**

It is a suitable next step after completion of the digital foundation 1 programme and as preparation for the upcoming digital foundation 2 programme.

Boxset episodes

During the interactive learning sessions you will work with a virtual partner and team. As the investigation unfolds, it becomes clear there is more to the initial incident than first thought.

Learners with a police force email address are encouraged to sign in to **Knowledge Hub** where you can find useful supplementary information to enhance your digital skills. **Watch our video** to find out how to sign up to Knowledge Hub, run by the Police ICT Company, and access our range of digital intelligence and investigation (DII) resources.

- Episode one: 'Digital Media – Internet of Things' provides basic digital advice and shows you how to identify which smart devices could be discovered.
- Episode two: 'Digital Scene Management' shows you how to secure and handle any devices needed for investigation and how to ensure that evidence is not corrupted, lost or deleted and the importance of the 'golden hour' scene preservation protocol and how to prioritise evidence.
- Episode three: 'Core Digital Data Collection' tells you how to search for social media evidence effectively, corroborate digital evidence from different sources, maintain the integrity of captured media and equips you with the best practice for witness submission of images, video and audio as evidence.
- Episode four: 'CCTV and ANPR' shows you how to establish the evidential value and limitations of CCTV, as well as the best-practice protocols surrounding CCTV seizure and access. You will learn how to collect and store CCTV security and surveillance footage correctly, finding out how to explain the legislative and procedural considerations prior to CCTV retrieval. You will get an understanding of the different purposes of CCTV and ANPR and the added value of ANPR to an investigation.
- Episode five: 'Core Digital Data Collation and Interpretation' runs you through how to interpret data from specialist units and understand when it is appropriate to seize a device. You will discover the non-specialist tools and techniques that you can use to collect, view and seize data from digital devices and understand how digital media investigators can help your investigation.
- Episode six: 'Digital Forensics' focuses on reviewing the evidence collected so far, and what forensic services might be used to help the investigation. It also covers the legislation and policy governing search and seizure, digital witnesses and device interactions.
- Episode seven: 'MISPERS' focuses on what digital opportunities there are to identify, locate and help trace a missing person. It also covers the 'golden hour' actions that the initial investigating officer should take, legislative authority, traceability tools and the levels of missing person

definitions.

- Episode eight: 'Online Fraud' covers identifying and investigating online fraud, including when to refer a victim to Action Fraud and the method that criminals can use – from phishing to dating scams.
- Episode nine: 'Internet, Intelligence and Investigation (III)' focuses on using the internet to gather information, intelligence and evidence as part of an III strategy.
- Episode 10: 'Digital Victims and Witness Support' shows you what immediate advice can be given and what initial safeguarding actions should be taken. Vulnerable groups may be more likely to become victims of digital crime and the episode shows how appropriate behaviours and attitudes should be applied to victims. 'The Verdict' summarises the operation and, depending on the answers to a set of questions, will determine how the prosecution of the case proceeds. Will the investigation produce a good outcome?

Sequel episodes

These four episodes will help you further develop your skills to protect witnesses and victims from digital threats.

- Episode one: 'Assessing risk and vulnerability in a digital environment' builds on the theme introduced in the boxset – missing from home – and focuses on the vulnerable Katelyn and her online relationship with a man called Sebastian. It covers the vulnerability assessment framework, the 10 risk principles, signposting to partner agencies, and your responsibility under the Victims' Code.
- Episode two: 'Maximising digital information and intelligence' follows on from episode one and shows how to make more use of the authorised professional practice on the extraction of material from digital devices during an investigation. This covers the 10 principles of extracting material from digital decides and addresses how technology can be used to maximise information in everyday policing.
- Episode three: 'Managing digital evidence' explores the management of digital crime scenes and looking for evidence that supports or disproves the case being investigated. It also concentrates on exploring the management of digital crime scenes and looking for evidence that supports or disproves child grooming charges.

- Episode four: 'Digital evidence as part of a case file' looks at building the case file for a charging decision. This includes applying national file standards, code tests and preparing material for a charging referral and disclosure. You will learn how to apply digital thinking and employ appropriate evidential processes when building a case file.

VAWG module

This module builds on the knowledge gained in the boxset and the sequel. It focuses on how to:

- recognise digital aspects of VAWG
- identify the potential digital indicators of abuse
- explain appropriate digital safeguarding opportunities

Digital crime and policing

The **Policing Vision 2025 plan** and a **'Real lives, real crime' report** from His Majesty's Inspectorate of Constabulary and Fire & Rescue Service (HMICFRS) both identified the effect that digital crime is having on policing. The reports also found a need for policing to better support and advise victims of crime and recommended better awareness of how to investigate and gather digital evidence.

Our interactive learning tool aims to tackle some of these recommendations and provide officers and staff with general digital policing skills so that they can respond appropriately to response calls: triaging the situation, protecting evidence and identifying if specialist support is needed.

Op Modify covers the digital subject areas that have been identified by policing as the priority areas for skills development. Give it a go.

Improve your digital thinking

All episodes of Operation Modify are available now through College Learn (you will need to log in to this).

- **Access the boxset via a secure computer**
- **Access the sequel via a secure computer**

- **Access the VAWG module via a secure computer**

Tags

Digital intelligence and investigation   Cybercrime   Managing investigations
Automatic Number Plate Recognition   CCTV