

Digital Media Investigator (DMI) role profile

Purpose	The Digital Media Investigator (DMI) is embedded within major investigation or serious organised crime investigation teams, rape teams and, if required by the LEA, can be deployed locally to support local investigation teams on volume crime. DMIs will collate and coordinate on all matters related to CD and other technology media. The DMI will obtain contributions from SPoCs, Digital Forensics, Open Source and other technology teams and support the related elements of analysis and case preparation. They will author the technology and data component of the overall operational strategy and ensure execution of the strategy in partnership with other stakeholders.
Key Outcomes Accountable For	<ul style="list-style-type: none"> ▪ Development of an effective technology and data strategy for investigation / operation ▪ Timely and effective input from SPoC, Digital Forensics, Open Source and ANPR/CCTV functions into investigation / operation to meet technology and data strategy ▪ Appropriate management of digital media within investigation / operation to meet prosecution needs, including development of appropriate evidence as well as disclosure of appropriate excess information
Main Responsibilities	<p>Development of technology and data strategies</p> <ul style="list-style-type: none"> ▪ Lead the development of the technology & data strategy (developed in conjunction with Analyst, SPoC, Digital Forensics, Open Source and other relevant technology functions and channelled into the overall strategy managed by the SIO) ▪ Lead in the development of a digital profile for a victim, witness or suspect on an investigation <p>Coordination of expert inputs</p> <ul style="list-style-type: none"> ▪ Coordinate returned digital media products with related products from ANPR/CCTV/Financial Investigation teams ▪ Co-ordinate the input of expert witnesses such as cell site engineers or RF technicians to support work around communications data ▪ Provide guidance to SIOs / Investigators on the application of technology in investigations / operations ▪ Take guidance and input from experts in SPoC Unit, Open Source, Digital Forensics and other technology teams and feed this into the investigative process ▪ Use these inputs to prioritise workload to be passed to the SPoC Unit, Open Source and Digital Forensics teams ▪ Coordinate meetings, discussions, planning and review sessions between SPoCs, Analysts, Open Source, Digital Forensics and ANPR/CCTV functions as part of the investigative or intelligence gathering / analysis process, including maintaining minutes, actions and keeping a record of all technology and data lines of investigation <p>CD acquisition and exploitation</p> <ul style="list-style-type: none"> ▪ Manage delivery against the technology and data strategy ▪ Where required, prepare CD applications on behalf of investigations or operations, with guidance from SPoCs, for submission to the SPoC Unit and/or support advanced TLOs in doing this ▪ Discuss, analyse and evaluate returned CD with Analysts, SPoCs and Investigators feeding the result into the investigative process in line with the technology and data strategy ▪ Liaise with major incident rooms (Receiver and Action Manager) on appropriate technology and data actions <p>Prosecution and disclosure</p> <ul style="list-style-type: none"> ▪ Work closely with Prosecutors (as well as the Analyst and SIO where applicable) on the technology and data elements of the case and the preparation of evidence, drawing on SPoC, Digital Forensics, Open Source and ANPR/CCTV other technology team expertise to ensure evidential files and products are fit for purpose

	<ul style="list-style-type: none"> Handle excess data appropriately, assess its impact on the case and take relevant action to ensure that it is passed to the Disclosure Officer where required in accordance with CPIA <p>Knowledge sharing and continual improvement</p> <ul style="list-style-type: none"> Identify and action opportunities for continual improvement in the input of SPoCs, Open Source, Digital Forensics in investigations, sharing these ideas using provided processes and systems (via the DMI Lead where one exists) Use agreed processes and systems to share knowledge and experience gained with CD users both within and across LEAs
Reports Into Skills	<p>Senior Investigating Officer (SIO)/Deputy SIO</p> <ul style="list-style-type: none"> Strong, competent investigative skills Ability to develop clear, concise articulate technology and data strategies Ability to complete a CD application form to the right level of detail for the type of request Ability to build strong working relationships with other teams e.g. Open Source, Digital Forensics, SPoC Basic skills in Excel and data manipulation / analysis e.g. filters and pivot tables Ability to use the LEA workflow system to submit applications Ability to present and communicate information clearly to all levels (both written and verbal) Ability to plan and prioritise high workloads with limited supervision Ability to challenge and influence the SIO, being able to successfully articulate the rationale behind the challenge Ability to apply RIPA and other legislation in practice to guide the acquisition of CD and other digital media Skills in management and coordination of multiple inputs from multiple individuals and teams
Knowledge	<ul style="list-style-type: none"> Remain up to date on the techniques used by SPoCs, Analysts, Digital Forensics and Open Source teams through networking with these teams and other DMIs and understand how these techniques can be applied together and the possibilities / limitations of using them Understand the application of ANPR, CCTV and financial analysis to support digital media investigations A strong knowledge of RIPA and its applicability to investigations/intelligence operations Understanding of non-RIPA data available Knowledge of different technology and data types Strong understanding of investigative and prosecution processes and how to prepare cases / evidence Knowledge of disclosure procedures and CPIA Good understanding of the PII Process and procedures relating to sensitive methodology (not LI) Knowledge of the grading system for CD Understanding the implications of retaining CD and other media for intelligence purposes and the implications for its use as evidence in subsequent investigations and prosecutions Knowledge of how CD and other media can be used as evidence to show corroboration, correlation, common purpose, chronology, similar fact evidence, presence etc Knowledge of emerging technology, trends and how it impacts on data acquisition and media collection Knowledge of exhibits management and how to give evidence
Experience	<ul style="list-style-type: none"> Practical experience of working on a broad range of investigations, including some with a data and technology focus (Essential)

	<ul style="list-style-type: none">▪ Experience of working in an environment where networking is critical (Desirable)▪ Experience of influencing senior individuals (Desirable)▪ Experience of working on a Major Investigation Team/Serious Organised Crime Investigation Team or local Criminal Investigation Team (Essential)▪ Experience of utilising capabilities of SPoC / Open Source / Digital Forensics teams (Desirable)▪ PIP Level 2 trained police investigator (or equivalent accreditation in other LEAs) (Desirable)
Special conditions	<ul style="list-style-type: none">▪ An affinity and aptitude for communications technology▪ Completion of relevant training relating to the role of DMI such as Core Skills in Communications Data training course, Open Source / Digital Forensics awareness training etc▪ Attendance of any DMI CPD and refresher training, technology / media seminars / conferences and networking events▪ The role requires receiving an appropriate level of clearance and can be a police or civilian officer▪ The role may be full time for major crime cases, and will be a dedicated role within the team or part time alongside delivery of other responsibilities, depending on the LEA organisational model and resource availability