East Midlands Special Operations Unit

Job Description

Title - Digital Forensic Specialist

Post Number:	XS368
Grade /Scale:	PO32 £35,223 –£37,953 SCP 29-32
Weekly Hours:	37
Department:	Digital Intelligence and Investigations
Status:	Established
Responsible To:	Technical Team Leader
Responsible for:	None
Location Work base:	Vicinity of Junction 27 (of M1)
Job Role /Purpose:	To use appropriate digital forensic techniques to identify and acquire evidence and intelligence held on digital media, devices and within networks as part of criminal investigations. Maintain the integrity of evidence and findings, document processes and work within defined quality procedures. Provide tactical advice to reactive and proactive investigations in relation to secreting digital evidence. Provide technical evidence for legal proceedings. Undertake research to develop advanced technical capabilities. Due to the nature of vetting clearance required for this role you must have 5 years continuous residency in the UK.
Health and Safety:	To comply with the health and safety policy and it's associated procedures and cooperate with your manager and the fore to protect your health and safety and that of other people. To comply with the relevant risk assessment for your job role and report accidents, incidents and near misses.
Contacts:	Police officers and police staff; Senior officers of the EMSOU and regional forces; external agencies; CPS, barristers and Judges; technical experts; industry and academic partners; quality management professionals and accreditation agencies.
Equality and Diversity	Actively advance diversity /equality, work towards eliminating discrimination, harassment and victimisation and foster good relations between all groups of people.

Person Specification

Knowledge, Skills & Abilities

Essential Criteria
A clear definition of the necessary criteria.

Knowledge/ Education (including qualifications):

- To be educated to degree level in a digital forensic, computer science or technical discipline or have work experience at this level.
- Have working knowledge and extensive experience in the use of industry tools such as Encase, FTK, NUIX, UFED, XRY, AXIOM or similar in the analysis of computers, storage devices, mobile devices and networks.

Work Experience:

- Experience and proficiency using a wide range of key technologies including advanced data extraction techniques in a digital forensic environment.
- Have experience of working within a team and independently, using your own initiative with discretion techniques in digital forensics.
- Experience of critical thinking and decision-making whilst under pressure and development of digital forensic strategies with a clear articulation of costs, benefits, risks, timescales, necessity and proportionality in response to specific investigative problems.

Personal / Interpersonal Skills, Aptitudes:

- Able to communicate technical issues effectively (both written and verbally) to technical and non-technical staff or stakeholders with the ability to pay close attention to detail and construct clear and appropriate recommendations.
- Experience and ability to deal with material (including images, videos and written content) of an unpleasant, disturbing and/or graphic nature; able to produce detailed and comprehensive reports of the contents.
- Able to apply methodical and creative approaches to problem solving and evaluate, prioritise and respond to changing operational situations with the ability to rapidly absorb new technical information.
- Experience working within a forensic environment that adheres to ISO 17020 and 17025, working to technical and quality management procedures, including performing roles or functions which are essential for the maintenance of accreditation as Technical Manager, Auditor or Assessor.

Special Skills:

- Experience of designing and conducting research in relation to key technical issues or concepts.
- Have a full UK driving licence and use of own vehicle for business use*

Other:

- Have a flexible approach to working, with a willingness to react to duty changes at short notice and provide occasional out of hours support to meet operational needs.

** Reasonable adjustments will be considered under the Equalities Act 2010.*

Desirable Criteria
Where available, elements that contribute to improved / immediate performance in the job.

Knowledge/ Education (including qualifications):

- To be educated to post-graduate level in digital forensic, computer science or technical discipline or be able to demonstrate equivalent work experience to this level.
- To be certified in the use of one or more digital forensic techniques or software applications.

Work Experience:

- Have knowledge and the practical application of relevant legislation such as Compute Misuse Act, Criminal Procedure, Investigations Act, Police and Criminal Evidence Act, Regulation of Investigatory Powers Act.
- Experience of collecting and analysing large digital data sets to provide meaningful insights to investigators.
- Have advanced skills in one or more key technologies such as coding/ scripting, database software and technology, computer and mobile operating systems, cloud services or servers and networks.
- Have a good understanding and practical application of NPCC/ACPO principles of digital evidence.

Personal / Interpersonal Skills, Aptitudes:

- Experience of creating and delivering presentations to varied audiences to convey technical concepts and findings.
- Experience of preparing and presenting evidence in legal proceedings.

Special Skills:

- Have a working knowledge of covert policing techniques in a technical environment.

** Reasonable adjustments will be considered under the Equalities Act 2010.*

Core Responsibilities/ Accountabilities

Operational:

Carry out forensic examination of digital devices, media and networks to secure, retrieve and report on the significance of data in accordance with the national and local guidelines, utilising a range of tools and techniques within an ISO 17025 and 17020 quality framework and adhering to ACPO principles of digital evidence.

Provide specialist expertise at scenes in relation to the recovery and where required examination of digital devices, media and volatile data. Support investigating officers with relevant technical knowledge when required in suspect or witness interviews.

Design, document and implement comprehensive digital forensic strategies in response to customer requirements from across a range of EMSOU departments and partner agencies. Provide clear and appropriate advice and negotiate work to be undertaken considering necessity, proportionality, collateral intrusion and disclosure. Make effective and appropriate decisions in respect of examination methodologies considering capacity, cost, data quality and risk.

Extract, process and Interpret digital data into a format suitable for investigators to examine for evidential or intelligence value. Use standard and bespoke processes to make sense of digital data, developing and validating new methods where necessary.

Prepare reports and statements of evidence in respect of digital forensic examinations undertaken and attend court or other statutory hearing as a witness when required. Provide specialist technical knowledge to assist the court in understanding the significance and relevance of digital evidence, communicating with investigators, CPS, defence experts and judges.

Work within the quality frameworks of IS0 17025 and 17020 undertaking necessary roles and responsibilities to maintain and advance accreditation. Tale an active role in the continuous improvement of the unit through processed such as regular peer review, assessment and auditing.

Undertake any other reasonable tasks commensurate with this role and its level of responsibility.

Management/Leadership:

Accept and promote personal responsibility for the maintenance and development of process and procedures required for an accreditation and the implementation of best practice with the unit and across EMSOU in respect of digital investigation.

Provide technical leadership in respect of continuous improvement within the unit, advancing technical investigations and data interpretation and identifying and developing new tools and techniques through creative innovation.

Communication:

Communicate technical concepts to a range of customers and stakeholders including Chief and Senior Officers, investigators and intelligence officers, other technical staff including law enforcement, industry and academic partners, the Crown Prosecution Service (CPS), barristers, defence experts and Judges, quality management professionals and accreditation bodies.

Produce comprehensive reports relating to date recovered from digital investigations, providing structured and clear recommendations and conclusions. Prepare and present evidence in court

in a clear and intelligible manner so that a non-technical audience can understand the significance and value of digital evidence.

Help prepare material for and attending training events to give instruction on matters related to digital investigations and intelligence (DII) and the recovery of digital evidence to technical and non – technical staff. Engage with internal and external agencies to deliver training, awareness and advise as and when required.

Liaise with other DII, digital forensic and technical units with law enforcement, as well as in industry and academia to exchange information and advance digital investigation, ensuring best practice is adopted and duplication minimised.

Administration:

Maintain full operational records which can be audited by both internal and external reviewers across all aspects of work undertaken in relation to digital investigation, adhering to legislation and polices on data retention, disclosure, date security and confidentiality.

Update and maintain technical knowledge through training, current case law, procedural rulings and developments concerning relevant issues and be able to document this on your training records.

General:

Actively promote equality of opportunity, work towards eliminating discrimination and promote good relations between all groups of people.

This role description will develop along with the changing demands of policing reflected in EMSOU priorities and should be reviewed every year as part of an induvial Professional Development Review (PDR) and the role requirement within ISO 17025 and 17020.

Be flexible in terms of working location and be prepared to work temporarily at other locations with the region and on occasions working outside of region.

** Reasonable adjustments will be considered under the Equalities Act 2010.*

Personal Values /Competencies

The competency and values framework sets out nationally recognised behaviours.

The framework has 6 Competencies – each competency can be split into 3 levels to fit around policing and non policing roles see here : Competency and Values framework

We analyse critically
We are innovative and open-minded
We are emotionally aware
We take ownership
We are collaborative
We deliver, support and inspire

All competencies are underpinned by 4 Values that should underpin everything that we do :

Integrity
Impartiality
Transparency
Public Service

Other

Security Check Levels refer to vetting for the specific levels that relate to this job role:

1) Management Vetting (MV)

2) Security Check (SC)

Due to the nature of vetting clearance required for this role you must have 5 years continuous residency in the UK.

Date line manager checked vetting level needed :

Car User: Yes - Essential /Casual Allowance *{per mile / day etc}:* Casual