Job Evaluation Numbers	A293 B802 B863

JOB DESCRIPTION

Job Title: Digital Forensic Investigator / Digital Forensic Investigator SEROCU / Digital Forensic Investigator CTPSE	**Location:** Various
Job Family: Business Support	**Role Profile Title:** BB3 Police Staff
Reports To: Unit Supervisor/Manager	**Band level:** Linked grade 3R-3S
Staff Responsibilities (direct line management of): Nil	

a. **OVERALL PURPOSE OF THE ROLE**: Defines the role, put simply, why it exists.

The overall purpose of the role is to: Conduct detailed forensic digital examinations as part of investigations and operations. Recover evidential data from computers, mobile devices, CCTV systems, the cloud and other electronic devices in accordance with the standing ACPO guidance and ISO17025 accredited investigative techniques. Gather and distribute relevant / quality intelligence and provide high quality written and oral evidence. Provide technical advice and assistance regarding all aspects of digital evidence to investigating officers, staff and partners engaged in the investigations.

b. **KEY ACCOUNTABILITY AREAS**: Define the important aspects of the role for which the job holder is responsible for results or outcomes.

The key result areas in the role are as follows:

1. Working to ISO 17025 standards conduct forensic digital examinations of seized computers, mobile phones and other electronic devices using appropriate processes, methodologies, tools and techniques, in accordance with ACPO guidance and court approved investigative techniques. Assess all immediately available electronic evidence, conduct risk assessments, assess the factors likely to impact on the investigations and check the necessary authorisations. Ensure all submitted items are under necessary authorisation and that exhibit continuity/management procedures are adhered to. This includes the retention and recording of all material for use as part of the investigative process.

2. Support investigations and prosecutions by providing written and oral evidence that can be presented to Officers in the Case (OIC), the Crown Prosecution Service (CPS) and Barristers to be given as testimony at Court as an expert witness (as indicated by judiciary). Manage the needs of customers and ensure simplification of evidence to ensure it is fully understood by those that have limited technical forensic knowledge.

3. Attend searches of premises to assist in the seizure and ‘live’ examination of computer exhibits including those with encrypted drives or containers, mobile devices and other digital equipment in line with ISO17020 standards. The live capture of computer RAM and use of command line functions to extract and analyse the recovered data in an evidentially secure manner. Identify and secure digital evidence sources to assist with investigations. Identify and mitigate Health and Safety risks associated with electronic devices. Utilise proprietary and bespoke forensic hardware, software and complex investigative techniques.

4. In accordance with legislation and policy assist in open source internet investigations and the capture / recovery of data from the internet and Cloud based services. Identify further investigative opportunities such as identifying suspect(s), victim(s) and potential witnesses. Develop techniques or applications for the recovery of data from unusual devices such as games consoles and the recovery of the associated cloud or platform data associated with their use. Recover data associated with the use of cryptocurrency to facilitate the recovery of funds. Understand and extract data relating to the use of the Dark Web and provide in an evidential format for use operationally.

Job Evaluation Numbers	A293 B802 B863

5. Maintain knowledge of current changes in technology and innovation in order to effectively support investigations and enhance the Digital Forensic service for the Force. Undertake independent research, (e.g. developing testing methodologies for new tools and products), personal development training and liaise with other forensic practitioners through professional organisations and forums.

6. Contribute to the effective and efficient running of Digital Investigations. Support the administrative processes for ISO 17025/17020 and carry out regular checks, equipment verification, software validation and maintenance on equipment held by the Digital Forensic Unit to ensure it remains operational. Apply quality assurance methods and reviews to ensure product produced is to the required standard to adhere to ISO17025 accreditation and FSR codes of conduct and practice. Deal with telephone enquiries in relation to all technical and administrative issues and assist in providing statistical information on the unit's performance and achievements.

7. Attend case conferences and provide expert advice and guidance to investigating officers and prosecutors in relation to evidence from computers, other digital devices and the Internet including urgent operational requirements whilst on call and writing of the Digital Forensic strategy for the case. Offer advice and address issues raised by defendants and defence experts to affect the decisions impacting investigation outcomes.

8. Evaluate and report electronic evidence in relation to criminal or civil investigation or to due diligence and maintaining professional standards. Identify further limits of examination as necessary and identify opportunities for further investigation if they exist.

9. Perform advanced technical examinations including JTAG, eMMC and Chip-off.
Good practical knowledge and skills in software development methodologies and techniques intended to facilitate the structured development of bespoke applications utilising programming languages such as Python, C++ and other scripting mechanisms.

10. Develop, test and document new and amended software solutions in accordance with high level solution designs and agreed standards that are capable of meeting defined business needs for Digital Investigations. Implement and maintain high quality, resilient and performing Forensic network systems including domain administration tasks.

11. Data analysis and interpretation of multiple data types such as hexadecimal to ensure data integrity and accuracy. Reverse engineering of software to analyse its functions and abilities, leading to accurate representation of recovered data for court presentation. This may include tasks such as the virtualisation of computers and mobile devices through platforms such as Virtual Box, VMWare or Android Studio.

12. Able to prepare, present and where possible provide the clarification of both audio and video product for review. Where necessary provide media presentations for court in order to ensure the best representation of the evidence available. Ensure all data recovered and identified is recorded and stored in a manner that maintains continuity and evidential integrity.

CTPSE Digital Forensic Investigators:
In accordance with national guidelines and policy, assist as required with specialist CCTV work such as the downloading of video and audio product from CCTV systems in commercial and private premises.

Job Evaluation Numbers	A293 B802 B863

c. **DIMENSIONS**: Include matters such as key result areas that make the greatest demands on the role holder, seasonal pressures, items processed, the number of customers and/or level of authority to make financial decisions or commit other resources.

Further Comments:
It should be noted that the nature of the role will expose the job holder to high volumes of extremely distressing material. The role holder will be expected to undertake regular psychological screening.
The role holder will have a high investigative/examination workload and will be responsible for managing the digital aspects of on-going investigations and need to be aware of how this interlinks with the bigger Criminal Justice picture.. They will be working to strict timescales and deadlines using a number of complex digital forensic tools and bespoke software packages.
The post holder must be willing to work flexible hours to suit the requirements of the department and must be willing and able to travel for business purposes to different locations across the force and undertake all assignments in a timely manner. The post holder will be expected to be part of an on-call rota and also be able to work some evenings and weekends where required. Due to these requirements a full UK driving license is also considered essential. **CTPSE & SEROCU Digital Forensic Investigators:** Must be willing to travel to different location across the force and the national CT/ROCU Network.
TVP & SEROCU Digital Forensic Investigators: The vast majority of work is related to very serious high risk crime and currently 85% of the cases examined in the unit relate to crimes committed against the most vulnerable in our society; including Child Sexual Exploitation, Indecent Images of Children and Organised Crime. In certain cases, particularly those involving Indecent Images of Children, the DFU provide the sole prosecution evidence. This often means the DFU member of staff is the key prosecution witness thus the quality of the evidence could directly impact whether a suspect is convicted or acquitted.

d. **CHARACTERISTICS OF THE ROLE**
Expertise: Concerned with the level of administrative, professional and/or technical expertise (knowledge and skills) needed to perform the role effectively; may be acquired through experience, specialised training, and/or professional or specialist education and training.

The knowledge or skills required in the role are as follows (essential or desirable): (Entry Level – Role holders will generally be tutored at this level)	***E/D***
1. Previous experience in a Digital Forensic environment including experience of exhibit handling procedures and giving evidence in court. Demonstrating a working knowledge of Digital Forensic techniques and software tools across a wide range of hardware and operating systems. Knowledge or experience of working within a quality system and meeting the requirements of the FSR Codes of Practice and Conduct.	E
2. Proven ability to work unsupervised/prioritise workload in order to meet deadlines and manage demands, frequently working under pressure sometimes dealing with distressing/disturbing material.	E
3. Proven knowledge and experience of a wide range of computer hardware/digital devices (mobile phones, software/operating systems and networks. Demonstrable experience of, or willingness to, investigate and analyse considerable amounts of data; focusing on potential and relevant evidence.	E
4. A good communicator – confident and assertive when required - who is able to deal with people at all levels both internally and external agencies, as well as working well in a team. Reducing highly technical issues into an easy to understand format. Whether within the team	E

Job Evaluation Numbers	A293 B802 B863

or with colleagues from other law enforcement agencies and external providers or advising colleagues, senior officers, barristers and the Judiciary.	
5. Proven ability to maintain accurate contemporaneous logs and records in a manner that can be easily retrieved by others. Good written skills/previous experience of provision of statistical information to a high level of accuracy, with a methodical approach and ability to analyse and produce solutions to problems.	E
6. Previous experience of computer/mobile phone forensic techniques/software e.g., XWays, Axiom, Cellebrite, XRY, GrayKey etc.	E
7. Previous experience in law enforcement/investigative organisation/s.	E
8. Able to recognise sensitive information and maintain discretion and confidentiality. Maintain a high degree of integrity and trust when dealing with sensitive and Government Security Marked information	E
9. The post holder must be willing to work flexible hours to suit the requirements of the department and must be willing and able to travel for business purposes, regionally and nationally. Full UK driving licence.	E
10. Familiar with database structure and configuration for formats such as SQL, SQLite, ESE, plist and XML.	E
11. Successful completion of the Core Skills in Data Recovery & Analysis/ Core Skills in Mobile Phone Forensics or industry equivalents.	E
12. Vendor-specific foundation level courses e.g. AccessData Bootcamp, XRY Foundations etc.	E
CTPSE Digital Forensic Investigators: The post holder must be prepared to undertake specialist training to assist with incidents involving Chemical, Biological, and Radiological or Nuclear (CBRN) materials in the United Kingdom.	E

The knowledge or skills required in the role are as follows (essential or desirable): <u>Experienced level</u> (Requires entry level skills to progress on to this level)	***E/D***
1. Proven and documented experience in the full Digital Forensic Investigator role and evidence of managing the digital part of on-going investigations and how this interlinks with the wider criminal justice picture. Leading on the direction of digital strategy for the investigation in conjunction with the OIC.	E
2. Capable of imparting specialist advice and knowledge and mentoring in the field of Digital Forensics to fellow colleagues, both in the team and the wider Force personnel.	E
3. Ability to demonstrate commitment to continuous professional development by identifying and undertaking independent technical and operational CPD and on-going competency based training and development.	E
4. Tutoring of new staff to develop skills under the Digital Forensics Competency Framework	E
5. Attendance at advanced level Digital Forensic training for Windows and Apple Forensics	E
6. Proficient in one or more application development software tools and languages such as C++, C# and Python	E