KENDALL COUNTY
OFFICE OF THE SHERIFF
Dwight A. Baird, Sheriff
1102 Cornell Lane Yorkville Illinois 60560
Phone: 630-553-7500 Fax: 630-553-1972
www.kendallcountyil.gov/sheriff

KENDALL COUNTY SHERIFF'S OFFICE
DIGITAL FORENSIC EVIDENCE, DATA, AND CRIME ANALYST (NON-SWORN)
JOB DESCRIPTION

The following statements are intended to describe the general nature and level of work being performed. They are not intended to be an exhaustive list of all responsibilities, duties and skills required of personnel so classified. This job description is subject to change as the needs and requirements of the job change.

GENERAL SUMMARY

To serve as the Digital Forensic Evidence, Data, and Crime Analyst; the employee will perform electronic evidence and data processing to assist deputies and investigators with the investigation, analysis, and processing of digital or electronic evidence. In addition, this employee will use a set of systematic, analytical processes directed at providing timely and pertinent information relative to crime patterns and trend correlations to assist operational and administrative personnel in planning the deployment of resources for the prevention and suppression of criminal activities, aiding the investigative process, and the clearance of cases. The Crime Analyst will work with staff to assist with projects as directed, be responsible for performing specialized administrative or investigative work, and coordinate with various units or personnel within the agency.

The position of Digital Forensic Evidence, Data, and Crime Analyst reports to the Investigations Sergeant and is a Fair Labor and Standards Act non-exempt position. This positon is not part of a bargaining unit.

PRINCIPLE DUTIES AND RESPONSIBILITIES:

- Identify, process, analyze, and report on a wide variety of digital and electronic evidentiary items.
- Utilize technical knowledge, training, and experience to assist deputies and investigators with digital and electronic evidence.
- Create a variety of reports, such as crime or police call maps. Empirical information will be collected, evaluated, and published to departmental units.
- Develop and analyze a variety of data sources, including departmental data sets, open source information and social media.
- Support the Investigations unit with the use of quantitative and qualitative methodologies such as link analysis, event flow analysis, hot spot mapping, and spatial analysis for the identification of specific criminal activity or crime patterns. Assist with pre-employment

background queries. Handle physical and digital evidence in legal and judicially acceptable manners.
- Liaise with law enforcement, government agencies, and community groups to obtain and/or provide crime-related data.
- Produce data analysis and reports to assist in staffing/resource allocation, and budgeting.
- May be required to testify in court and travel to crime scenes.
- Perform other duties as assigned or as necessary in the efficient and effective performance of the job functions.
- Provide courtroom testimony related to cases.

ENVIRONMENTAL FACTORS:

- Job functions will typically be conducted within an office setting. However, the Crime Analyst may be required to be present at crime scenes to complete these functions.
- The noise level in the work environment is typically low to moderate.
- While performing assigned job duties, employee may be exposed to files, documents, videos, and photographs of a graphic or sexual nature.
- Employee must be able to perform all assigned job duties during normal business hours but may be required to work during off-business hours during emergencies, or time sensitive situations.
- Employee must comply with KCSO policy and procedures, all other directives, and lawful orders.
- This is an on-site, in office position will some field work.

EQUIPMENT:

The position requires the ability to operate the following equipment:

- Computer; laptop desktop, or other forms of computer or electronic devices; cellular phone, criminal justice information terminals, general office equipment, fax machine, vehicles, hand and power tools necessary for use on electronic devices, any other specialty equipment necessary to complete digital forensic analysis.

QUALIFICATIONS

Education and Experience:

- An associate's degree from an accredited college or university.
- Two (2) years' experience in a field such as statistical analysis, computer science, computer or cellular forensics, information technology, criminal justice, business administration or public administration.
- Ability to obtain core certifications in computer, digital, or cellular forensics within the first year of hire. Additional certifications may be attained as budgetary and staffing constraints allow.

Knowledge, Skills and Abilities:

- Knowledge of computers, cellular phones and other related applications.
- Knowledge of Microsoft Office, GIS application software, database software and record management systems.
- Knowledge of proper methods of intelligence information gathering.

- Effective writing skills to compose, compile and maintain reports in writing so that the product is timely, accurate and understandable to others.
- Time management skills to manage and organize thoughts, information and resources into a logical sequence or workable plan of action.
- Must obtain CCO, CCPA, CCME within the first year, and;
- Have the skills and capability to obtain certification in computer or cellular forensics. (e.g., CFCE, GCFE, EnCE, MCFE, GASF, CCCE, CCRS). This list in not all inclusive and additional certifications may be required to fulfill job duties as technology and systems change.
- Ability to present ideas clearly and concisely both verbally and in writing.
- Ability to interact with others in a professional and business-like manner.
- Ability and willingness to adapt to changing circumstances and needs as the situation necessitates.
- Ability to work independently, with minimal supervision and strong decision making skills.
- Ability to understand and follow through on verbal or written instructions, and to accurately relate instructions in full or in part to other staff.
- Ethical and professional conduct, utilizing discretion, sound judgement, fairness, respect and integrity.
- Accountability for the information and data being handled.
- Ability to prepare accurate and comprehensive reports.
- Possess and maintain a valid driver's license.

JOB DESCRIPTION APPROVAL:

I have reviewed this job description and understand that it reflects the major tasks of my job. If I have any questions, I understand I can contact my supervisor.

_____ _____

Employee's Signature and Badge Number *Date*

I have issued this job description to the employee.

The job description currently reflects the needed skills and abilities required to perform the job of Digital Forensic Evidence, Data, and Crime Analyst.

_____ _____

Commander's Signature and Badge Number *Date*

Attachment: Summary of Certification Definitions.

Certifications defined per the certifying entity or vendor:

Certified Forensic Computer Examiner (CFCE) certification program is based on a series of core competencies in the field of computer/digital forensics.

The GIAC Certified Forensic Examiner (GCFE) certification validates a practitioner's knowledge of computer forensic analysis, with an emphasis on core skills required to collect and analyze data from Windows computer systems.

GIAC Advanced Smartphone Forensics (GASF)

The EnCase™ Certified Examiner (EnCE) program certifies both public and private sector professionals in the use of Opentext™ EnCase™ Forensic. EnCE certification acknowledges that professionals have mastered computer investigation methodology as well as the use of EnCase software during complex computer examinations.

MCFE certification is an accreditation that showcases an examiners' expert-level competence with Magnet Forensics products to peers, internal stakeholders and external audiences, including legal teams or clients.

The Cellebrite Certified Operator (CCO) course is a 2-day intermediate level certification program which builds on the CMFF course concepts. This course is designed for participants tasked with extracting data in a forensically sound manner using UFED Touch or UFED 4PC.

The Cellebrite Certified Physical Analyst (CCPA) course is a 3-day advanced level program designed for technically savvy investigators, digital evidence analysts and forensic practitioners. As this course focuses on the analysis and advanced search techniques using Physical Analyzer, participants will not be conducting extractions from devices in this course. Physical Analyzer software will be used extensively to explore recovered deleted data, database contents, advanced search and analysis techniques, verification and validation, and reporting.

he Cellebrite Certified Mobile Examiner (CCME) track is designed to prepare practitioners with the knowledge, skills and abilities of mobile device forensics and investigations.

The Cellebrite Certified Computer Examiner (CCCE) track is designed to prepare practitioners with the knowledge, skills and abilities of computer device forensics and investigations. These course tracks also prepare the candidate to utilize Cellebrite's Digital Collector and Inspector technology to conduct extractions, analyze findings, and prepare reports for legal proceedings.

The Cellebrite Certified Recovery Specialist (CCRS) track is a hardware-based track designed to prepare practitioners with the knowledge, skills, and abilities to identify potential electronic evidence, properly collect data and extract data on multiple digital devices – including smart devices, vehicle GPS, drones, IoTs, and many others. These course tracks also prepare to recover destroyed or encrypted evidence using destructive and non-destructive methods.