



# Charles County Sheriff's Office



To perform this job successfully, an individual must be able to perform the essential job functions satisfactorily. Reasonable accommodations may be made to enable individuals with disabilities to perform the primary job functions herein described. Since every duty associated with this position may not be described herein, employees may be required to perform duties not specifically spelled out in the job description, but which may be reasonably considered to be incidental in the performing of their duties just as though they were actually written out in this job description.

## DIGITAL FORENSIC ANALYST

<b>Division:</b>	<b>Criminal Investigations</b>
<b>Section:</b>	<b>Investigations</b>
<b>Pay Grade:</b>	<b>116</b>
<b>FLSA Status:</b>	<b>Non-Exempt</b>
<b>Classification:</b>	<b>Full-Time</b>
<b>Updated on:</b>	<b>June 2023</b>

### **JOB SUMMARY**

This critical position identifies, recovers, analyzes and formats data from a variety of digital sources, including cell phones, computers and databases, and provides this information to investigators, in a relatable and relevant format. Data recovery and analysis includes generating cell phone mapping reports and searching law enforcement databases for relevant information. It includes the ability to translate and explain the significance of highly-technical data into less-technical terms to ensure clear understanding for anyone who needs the information to include testimony in court. This position includes the recovery of data from mobile devices with an emphasis on locating data relevant to an investigation in various data sets and providing this information to detectives quickly.

### **ESSENTIAL JOB FUNCTIONS**

- Maintains the ability to utilize the latest technology and tactics to investigate and examine digital devices.
- Provides technical support for the identification, protection, preservation and collection of evidence at complex or major crime scenes.
- Conducts comprehensive forensic examination of computers, cell phones and other digital media.
- Examine cell phones in a forensically sound manner with the purpose of identifying, preserving, recovering, and analyzing evidence.
- Follow processes and procedures in retrieving, recovering, and preserving electronic evidence.
- Extracts, stores and analyzes data for evidentiary value in all types of investigations.
- Maintains necessary certifications for digital forensic analyst.
- Provides analysis of subpoenaed and seized documents and communication devices.

- Performs telephone toll analysis and document results in investigative reports.
- Identifies the user of cell phones by querying numerous secure on-line databases and evaluating information found.
- Corroborates witness testimony with telephone calling data.
- Briefs local prosecutors, management officials, detectives, and task force officers on support status of an investigation.
- Obtains subscriber information and telephone calling data via subpoena and/or court orders.
- Provides guidance, advice, and direction to police officers, detectives, supervisors and command staff in relation to the collection and preservation of electronic evidence.
- Assists officers and detectives with the proper collection of digital media.
- Collects, examines, and reports on digital media.
- Edits video as needed for court purposes or media presentations.
- Maintains a working relationship with counterparts in neighboring jurisdictions to ensure proper awareness to industry standards.
- Conducts technical examination of digital audio & video files recorded in different formats and using different CODECs and containers.
- Maintains computers and lab equipment.
- Conducts validation testing on computer forensic equipment.
- Conducts thorough examinations of computer drives, mobile devices, optical media, and other electronic data storage media.
- Preserves and copies the original media.
- Assists with Internal Investigation cases and administrative cases, as needed.
- Prepares and presents findings, provides expert testimony.
- Works with prosecutors and others to prepare cases for trial.
- Works to safeguard all devices from external intrusion and maintains security of digital forensic lab.
- Provides technical support to police officers.
- Trains and instructs other employees in safe collection and handling of digital devices and media.
- Assists officers and detectives with drafting of Search Warrants, Court Orders, and Subpoenas related to digital media.
- Maintains the appropriate software licenses and upgrades for the forensic tools necessary to complete forensic examinations.
- Receives, documents, and processes evidence collected by other members of this Agency.
- Labels, collects, transports and secures evidence from crime scenes.
- Recovers and preserves evidence from crime scenes, suspects and victims using proper techniques as outlined in various written directives of this Agency, as well as multiple federal regulatory agencies.
- Transports and maintains accurate chain of custody of forensic evidence to other federal, state, and local agencies.
- Documents investigations with photographs, recovery of physical evidence, and sketches of crime scenes.
- Prepares written reports and work assignments in a timely and efficient manner.
- Maintains accurate documentation for all cases worked.
- Gathers information, writes notes, reports, and other documents necessary to provide the State's Attorney with information needed for the prosecution of cases.
- Testifies in court and at other proceedings in a clear, well-organized, and logical manner describing events, objects, processing methods, and evidence associated with a case.
- Performs preventive, and required maintenance on assigned Agency vehicle.
- Attends and participates in meetings and training sessions, as required.
- Maintains archive of Interview Recording System.

- Develops the protocols and guidelines for the unit-based experience, training and best practices.
- Collects, examines and clarifies video surveillance from various locations within the County.
- Supports data sharing efforts with local authorities.
- Performs other related job duties as assigned.

## **QUALIFICATIONS**

### **Education and Experience:**

Bachelor's Degree in Criminal Justice, Digital Forensics, Computer Science or Related Field

And/Or

Law enforcement experience with skills associated with digital evidence extraction/analysis.

Any combination of these qualifications would meet the requirements

### **Licenses or Certifications:**

- Must possess a valid driver's license.
- Must be able to obtain the necessary data extraction and analysis certifications to perform the job duties during the early launch of employment.

### **Special Requirements/Qualifications:**

- Must pass a comprehensive background investigation.
- Must pass random drug screening.
- Must perform work in accordance with sound safety practices.
- Must report for duty in a regular and punctual manner.
- Must work overtime and work varying hours on a rotating schedule including days, evenings, midnights, weekends, and holidays, as required.

### **Knowledge, Skills and Abilities: Preferred, not Required**

- Knowledge of the principles and methods, rules and regulations found in the Standard Operating Procedures (SOP), and other manuals pertinent to the assigned job classification.
- Knowledge of the principles, methods and techniques used in the field of digital forensics.
- Knowledge of general operating systems software and of computer hardware.
- Knowledge of computer forensic software (i.e. EnCase, AccessData Forensic Software, Cellebrite, Oxygen, Magnet Forensics AXIOM, etc).
- Knowledge of applicable criminal laws, techniques, law enforcement reporting systems, law enforcement operations and practices.

### **Knowledge, Skills and Abilities:**

- Knowledge in the use of office equipment such as a calculator, computer, fax, and copy machines.
- Knowledge of the rules of evidence including the importance of chain of custody.
- Skill in making effective presentations before large or small groups and the ability to testify in a court of law.
- Ability to recognize evidence and know its potential value.
- Ability to think logically and apply deductive reasoning in solving problems.
- Ability to conduct examinations of digital media in a forensically sound manner.

- Ability to document investigations, including the recovery of physical evidence.
- Ability to work independently.
- Ability to communicate with others using nontechnical language to explain complex technical subjects.
- Ability to establish and maintain effective working relationships with user agencies
- Ability to safely lift and carry up to 50 pounds.
- Ability to operate an assigned Agency motor vehicle, both day and night, in all weather situations and road conditions in a manner to expeditiously, yet safely, arrive at a scene.
- Ability to learn names and locations of roads, buildings, and other landmarks in Charles County.
- Ability to utilize the senses of sight, hearing, smell, and touch.
- Ability to understand oral and written instructions, to speak effectively and articulately, to demonstrate good listening skills, and to convey concern, understanding, and empathy.
- Ability to read and comprehend a variety of legal and non-legal documents, maps, and reference material to properly comply with organizational rules and procedures.
- Ability to read, write, comprehend, and speak English in a clear, effective manner, using proper pronunciation, diction, and grammar.
- Ability to meet and deal effectively with Agency and government personnel and the general public.
- Ability to apply knowledge, experience, and reason to arrive at effective and logical decisions for routine situations.
- Ability to utilize a high level of discretion, good judgement, and confidentiality.
- Ability to maintain a high level of accuracy in assigned tasks.
- Ability to organize and determine priorities of diverse assignments.
- Ability to plan, organize, and effectively present ideas and concepts to groups.
- Ability to assimilate information from a variety of resources.
- Ability to analyze, evaluate, and select, often with limited information, the best course of action.
- Ability to write, compose, and develop documents, manuals, and other literature.
- Ability to read and comprehend various documents.
- Ability to maintain composure and work effectively in stressful situations of on.
- Ability to comprehend, understand, and adhere to, at all times, Agency policies, procedures, rules, and regulations.
- Ability to communicate effectively and coherently with other Agency personnel and the public, either in person or by telephone, by written report or memorandum, through radio communications or computer network.
- Ability to maintain proper care and maintenance of Agency equipment and facilities.
- Ability to perform vehicle maintenance, such as changing tires and checking fluids.
- Ability to function in a structured organization with strict rules of conduct.
- Ability to maintain professional decorum at all times.
- Ability to maintain effective working relationships with coworkers and supervisors.
- Ability to comprehend and retain old and new information, received both orally and in writing.
- Ability to appropriately accept supervision, criticism, and evaluation.
- Ability to maintain sensitivity to people from varying ethnic, religious, sexual, and socioeconomic backgrounds.
- Ability to deal tactfully, effectively, and equitably with people, both within and outside the Agency.
- Ability to comply with Agency policies and procedures as outlined in the Administrative and Operational Manual.

### **PHYSICAL DEMANDS**

The work is sedentary with frequent periods of reading, computer, phone and camera screens. Must be able to climb a step stool or stoop down to reach file drawers just above or below arm level, sit for prolonged periods of time, answer the telephone, and operate computer equipment by inputting and retrieving information, enter and exit motor vehicles frequently and quickly, respond immediately to calls for assistance, both on foot and by motor vehicle, manipulate keys and keyboards, file drawer latches, and file folders (locating, removing, inserting). Occasional tasks include climbing a ladder to access electronic devices in obscure locations.

### **WORK ENVIRONMENT**

Work is performed primarily in an office setting with frequent interruptions. There will be exposure to all types of environmental conditions, ranging from a courtroom setting to being at a crime scene for a prolonged period of time. Temperatures can range from below freezing to above 100 degrees. Work is performed while adhering to Universal Barrier Precautions when exposed to blood, body fluids, unknown chemical and bio-hazard conditions while on scene or processing evidence.