**Digital Forensic Examiner**

**Grade: 9**

**FLSA: Non-Exempt**

**Date: 07/22**

**Job Summary:** Perform critical work related to criminal investigations and other areas of law enforcement by acquiring electronically stored data and software on cellular devices and other computer-related materials. Work includes, but not limited to, acquiring, and analyzing cellular data on devices including cellular transaction records and call detail and geo location records, in a forensically sound manner, utilizing previously validated forensic hardware and software tools. Prepare and submit detailed reports for actions taken while maintaining chain-of-custody and ensuring the accuracy of information from the start of the investigation through court presentation. Examiners receive supervision from, and report directly to, the Crime Lab Supervisor. Work is evaluated through observations, conferences, and reports.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Essential Functions:**

1. Prepare non-evidentiary hardware and software utilized by verifying its performance and ensuring software is up to date.
2. Process and/or acquire digital media utilizing validated forensic hardware and software to forensically copy data found on electronic devices so that the integrity of original evidence is preserved.
3. Examine and/or analyze acquired data such as text, graphics, multimedia, and digital images utilizing various previously verified forensic software such as Cellebrite Physical Analyzer and Oxygen Forensic Detective.
4. Restore recoverable deleted data.
5. Access password-protected and secured data.
6. Verify the integrity of forensic copies used for analysis to ensure no data is lost or modified during the acquisition or copying process.
7. Interact with detectives, analysts, crime lab technicians, or outside professionals to acquire information necessary to perform forensic examinations.
8. Verify the correctness of the devices internal clock, if applicable.
9. Physically disassemble, examine, and reassemble devices, when necessary.
10. Identify evidence of crimes in which digital media and/or data was used and/or obtained.
11. Label and secure evidence per agency policy and procedure.
12. Maintain chain-of-custody of evidence.
13. Conduct detailed analyses of cellular and non-cellular communication records as provided by various communications providers such as CDR’s and geo location records.
14. Prepare detailed reports of actions taken and ensure the accuracy of information reported.
15. Properly archive any data obtained for retention purposes.
16. Train personnel on best practices for documenting and collecting digital evidence to ensure it is not damaged or lost.
17. Testify, as an expert witness, in court and at other proceedings in a clear, well-organized, and logical manner to accurately provide information describing evidence associated with a case.
18. May require:
    * Call back.
    * On-call.
    * Successfully passing proficiency tests.
19. Performs other duties as assigned.

**Required Knowledge, Skills, and Abilities:**

1. Ability to gain thorough knowledge of St. Mary’s County Government and Office of the Sheriff policies and procedures.
2. Ability to gain thorough knowledge of Crime Lab standard operating procedures as it pertains to digital forensics.
3. Ability to effectively communicate with agency and government personnel and the public, either in person or by telephone, by written report or memorandum.
4. Ability to recognize digital evidence and know its potential value.
5. Knowledge of techniques for recovering digital media to include understanding proper collection, processing, and preservation procedures for various types of digital devices.
6. Knowledge of basic computer functions and how data is stored.
7. Ability to properly and accurately document investigations, including the recovery of digital evidence in a detailed and articulate report.
8. Ability to work under pressure and prioritize casework with short deadlines.
9. Knowledge of various social media platforms such as Facebook, Instagram, Snapchat, etc.
10. Knowledge of chain-of-custody procedures when handling evidence.
11. Ability to utilize the senses of sight, hearing, and touch.
12. Ability to learn and operate a wide variety of forensic hardware and software.
13. Ability to understand and follow complex oral and written instructions, to speak effectively and articulately, to demonstrate good listening skills, and to convey concern, understanding, and empathy.
14. Ability to utilize a high level of discretion, good judgement, and confidentiality.
15. Knowledge of Microsoft Windows based computer programs to include the Microsoft Office Suite.
16. Ability to work independently and as a team on tasks and maintain complete and accurate records.
17. Knowledge of forensic techniques and ability to maintain currency on new and innovative techniques.

**Education and Experience:**

1. Associate’s Degree, preferably in Information Technology, Computer Science, or Computer/Digital Forensics.
2. Or three or more years of experience in Information Technology, Computer Systems Analysis, and/or data acquisitions on cellular devices.
3. Or any combination of equivalent technical training, education, and/or related experience.

Note: Experience performing digital data recovery and examinations on computers and/or cell phones may be substituted on a year-for-year basis for the required education.

**Additional Requirements:**

1. Possess a valid Maryland Driver’s License.
2. Ability to pass a comprehensive background investigation.
3. Ability to pass random drug screening.
4. Ability to pass polygraph examination.
5. Ability to satisfactorily complete assigned specialized and annual training to obtain and maintain various forensic certifications (Cellebrite, Oxygen Forensics, GeoTime, etc.)
6. May require availability for on-call or call back in extenuating circumstances.

**Physical and Environmental Conditions:**

1. Exposure to graphic, explicit, and disturbing images, sights, and sounds.
2. May be exposed to hazardous materials, illicit drugs, biohazards, and other contaminants.
3. May require occasionally utilizing a step stool or ladder, to reach above or below arm level.
4. May require occasional strenuous effort. For example, handling of moderately heavy boxes or evidence 20-50 pounds.
5. Requires long periods of computer-based tasks.
6. Requires long periods of sitting or standing.
7. Function in a structured organization with strict rules of conduct.
8. Requires occasional use of protective gear including, but not limited to, gloves and masks.
9. May require local travel.

The above job description is not intended as, nor should it be construed as, exhaustive of all responsibilities, skills, efforts, or working conditions associated with this job.

Reasonable accommodations may be made to enable qualified individuals with disabilities to perform the essential functions of this job.

I certify that this is an accurate statement of the essential functions and responsibilities of this position.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_

HR Representative Date

Your signature below indicates that you have received a copy of this position description.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_

Employee’s Signature Date