

State of Michigan  
Civil Service Commission

Capitol Commons Center, P.O. Box 30002  
Lansing, MI 48909

Position Code

1. SPDALTE

## POSITION DESCRIPTION

This position description serves as the official classification document of record for this position. Please complete the information as accurately as you can as the position description is used to determine the proper classification of the position.

<b>2. Employee's Name (Last, First, M.I.)</b>	<b>8. Department/Agency</b> STATE POLICE
<b>3. Employee Identification Number</b>	<b>9. Bureau (Institution, Board, or Commission)</b> Field Support Bureau
<b>4. Civil Service Position Code Description</b> Sp Digital Forensics Analyst-E	<b>10. Division</b> Intelligence Operations Division
<b>5. Working Title (What the agency calls the position)</b> Digital Forensic Analyst	<b>11. Section</b> Cyber Section
<b>6. Name and Position Code Description of Direct Supervisor</b> SMITH, WESLEY E; STATE POLICE DETECTIVE LT	<b>12. Unit</b> Computer Crimes Unit
<b>7. Name and Position Code Description of Second Level Supervisor</b> ELLIS, JAMES C; STATE POLICE FIRST LIEUTENANT	<b>13. Work Location (City and Address)/Hours of Work</b> 228 Magazine Street, Sault Saint Marie Michigan 49783 / M – F / 8:00 – 5:00

**14. General Summary of Function/Purpose of Position**

This position is responsible for completing forensic examinations of digital media and validation testing of computer hardware and software. This position conducts forensic investigations into computer related criminal activity including but not limited to the coordination and directing of forensic activities on computer-related equipment, networks, and information systems. This position is a technical consultant to federal, state, and local law enforcement agencies. This position assists in the development and implementation of computer forensic training programs. This position conducts investigations involving Internet and other technologies specifically incidents involving exploitation of children, and possession/distribution of Child Sexually Abusive Materials (CSAM). This position provides courtroom testimony for complaints investigated by the Computer Crimes Unit (CCU) and/or the Internet Crimes Against Children (ICAC) Task Force. This position is a member of the ICAC Task Force.

**15. Please describe the assigned duties, percent of time spent performing each duty, and what is done to complete each duty.**

**List the duties from most important to least important. The total percentage of all duties performed must equal 100 percent.**

**Duty 1**

**General Summary:**

**Percentage: 60**

Serves as forensic examiner by demonstrating knowledge and skill in the methods and techniques of conducting computer technology investigations and data recovery.

**Individual tasks related to the duty:**

- Reviews requests for forensic computer examinations and determines the type and methodology of examination needed.
- Responds in a professional and timely manner to quickly isolate and identify problems. Examines and explores all probable solutions in order to determine the best course of action.
- Conducts forensic examinations of computers and associated digital media. Utilizing experience gained to complete the most difficult forensic examinations and modifies systems, hardware, software, and diagnostic tools.
- Conducts examinations using a forensic data recovery software tools.
- Utilizes data retrieval utilities to accurately recover evidence and information from computers and related storage media.
- Prepares complete and accurate reports of the results of forensic examinations.
- Follows up on services by communicating with the requesting agencies to ensure that all data recovery needs have been met.
- Examines and analyzes all forms of digital media storage devices utilizing the Windows operating system, including, but not exclusive to computers, flash media, memory cards and mobile devices. Retrieves information stored on the device in a form useful to investigators and prosecutors. Identify, diagnose, and correct errors and problems. Ensures precautions are taken to prevent data and equipment damage.
- Knowledge and application of Operating Systems, Internet browsers, search engines, e-mail systems, and research tools.
- Initiate investigations subsequent to a report of activity involving the illicit use of computer-related systems and/or associated electronic data storage devices.
- Inspect and analyze computer hard drives, various software packages, decode passwords, identify encryptions and/or data via the use of software, uncover fraudulent use of the internet and/or email systems, including but not limited to cases of CSAM.
- Generates investigative correspondence consistent with departmental protocol.

**Duty 2**

**General Summary:**

**Percentage: 10**

Serve as a source of technological and consulting expertise to the local, state and federal law enforcement and criminal justice community as a means of ensuring the fulfillment of the department mission.

**Individual tasks related to the duty:**

- Develop and maintain a nationwide professional networking and informational gathering among peer agencies/units and the computer forensics community.
- Receive and respond to law enforcement inquiries requesting guidance and/or technical expertise/consultant.
- Assists local law enforcement agencies in preparation of affidavits and search warrants.
- Assist in the development of training courses for the law enforcement and criminal justice community of relevant classes, seminars, etc.
- Testifies in court at all levels regarding the results of evidence analysis and crime scene investigations.
- Responsible for providing technical evidence and assistance to local, state, and federal law enforcement agencies.
- Conducts vulnerability studies and validation studies on computer hardware, software and network systems used to conduct computer forensics and cybercrime investigations.

**Duty 3**

**General Summary:**

**Percentage: 10**

Maintain computer equipment and software vital to the day to day operation of the CCU statewide.

**Individual tasks related to the duty:**

- Maintain records of repairs, maintenance, preventative maintenance, upgrades, and modifications to equipment
- Manage and maintain servers and clients connected to the FLAN and the UCLAN.
- Recommend equipment purchases for repairs and upgrades as needed.

**Duty 4****General Summary:****Percentage: 10**

Maintains knowledge of current trends and developments in the field by reading appropriate literature and attending related training, conferences, and seminars. Applies pertinent knowledge to the performance of duties.

**Individual tasks related to the duty:**

- Maintains knowledge of most recent related court decisions and performs difficult forensic computer examination in accordance with those rulings
- Researches and keeps abreast of current developments in hardware, software, networks, operating systems and forensic data recovery equipment in order to ensure that the most current information and methodologies are utilized.
- Assists in development of new methods of analyses, as well as improvement and enhancement of digital forensic data recovery methods.
- Works with other forensic scientists, examiners, and information technology specialists in exploring and developing ways of conducting forensic examinations.
- Identifies, recommends, and conducts research and development of new or improved equipment, programs, methods and procedures.
- Attends conferences, seminars, and training courses as available for continuing professional education.

**Duty 5****General Summary:****Percentage: 5**

Assist with distribution involving Internet Cyber Tips involving the exploitation of children.

**Individual tasks related to the duty:**

- Assist the ICAC Task Force Commander in review of Cyber Tips from the National Center for Missing and Exploited that are assigned to the Michigan ICAC Task Force.

**Duty 6****General Summary:****Percentage: 5**

Assist in the prosecution of individuals associated with the illicit use of electronic data storage systems, and ensure the preservation of evidence.

**Individual tasks related to the duty:**

- Participate in crime scene searches via the examination of electronic data storage systems.
- Participates in on-the-scene investigations of major crimes, with local agencies.
- Participate in the drafting of search warrants.
- Preserve and package forensic evidence at crime scenes.
- Attend court and provide testimony on CCU and/or ICAC investigations.
- Assist in the preparation of court case exhibits and displays.
- Meet with officers and/or prosecutors in preparation for court cases.
- Assists with the seizure of computer related evidence, preparation of search warrants, and the preparation of investigative information for court purposes.
- Examine existing investigative strategies employed by the Computer Crimes Unit while comparing its effectiveness to state-of-the art applications used by counterpart agencies throughout the nation.

**16. Describe the types of decisions made independently in this position and tell who or what is affected by those decisions.**

- Manage forensic cases assigned.
- Determine through research materials cases to be investigated and the appropriate investigative/forensic methods or procedures to be utilized.
- Decisions of configurations of the UCLAN servers and systems that alter the interactive experience of users of computers attached to the LANs.

**17. Describe the types of decisions that require the supervisor's review.**

- Report and peer review.
- Equipment and software purchases.
- Approval of deviation from policy.
- When decision results in an impact to an agency's business processes.
- When the decision impacts systems or business units outside the governance of the CCU.

**18. What kind of physical effort is used to perform this job? What environmental conditions in this position physically exposed to on the job? Indicate the amount of time and intensity of each activity and condition. Refer to instructions.**

- The position operates in a normal office environment, performing duties within the assigned workspace.
- Tasks can be completed routinely seated at a desk, visiting others at their desks, in the context of meetings and meeting rooms.
- Work requires extensive use of personal computers including keyboards and monitors.
- This position is subject to stress and pressure to resolve problems quickly and effectively.
- This position is subject to long term effects associated with exposure to CSAM.
- There are frequent deadlines that are imposed by external forces; heavy workloads are possible and overtime for priority forensic examinations may be required.
- Duties generally involve lifting of 25 pounds or less.

19. List the names and position code descriptions of each classified employee whom this position immediately supervises or oversees on a full-time, on-going basis.

Additional Subordinates

20. This position's responsibilities for the above-listed employees includes the following (check as many as apply):

- |                            |                                    |                            |                                   |
|----------------------------|------------------------------------|----------------------------|-----------------------------------|
| <input type="checkbox"/> N | Complete and sign service ratings. | <input type="checkbox"/> N | Assign work.                      |
| <input type="checkbox"/> N | Provide formal written counseling. | <input type="checkbox"/> N | Approve work.                     |
| <input type="checkbox"/> N | Approve leave requests.            | <input type="checkbox"/> N | Review work.                      |
| <input type="checkbox"/> N | Approve time and attendance.       | <input type="checkbox"/> N | Provide guidance on work methods. |
| <input type="checkbox"/> N | Orally reprimand.                  | <input type="checkbox"/> N | Train employees in the work.      |

22. Do you agree with the responses for items 1 through 20? If not, which items do you disagree with and why?

Yes.

23. What are the essential functions of this position?

This position is responsible for completing forensic examinations of digital media and validation testing of computer hardware and software. This position conducts forensic investigations into computer related criminal activity including but not limited to the coordination and directing of forensic activities on computer-related equipment, networks, and information systems. This position is a technical consultant to federal, state, and local law enforcement agencies. This position assists in the development and implementation of computer forensic training programs. This position conducts investigations involving Internet and other technologies specifically incidents involving exploitation of children, and possession/distribution of Child Sexually Abusive Materials (CSAM). This position provides courtroom testimony for complaints investigated by the Computer Crimes Unit (CCU) and/or the Internet Crimes Against Children (ICAC) Task Force. This position is a member of the ICAC Task Force.

24. Indicate specifically how the position's duties and responsibilities have changed since the position was last reviewed.

Requesting to downgrade to the P11 level for recruitment and training purposes.

25. What is the function of the work area and how does this position fit into that function?

The assignment is within the CCU, Cyber Section. The CCU is an assisting unit that provides forensic and investigative support to all law enforcement agencies within the State of Michigan. The Michigan ICAC Task Force which investigates exploitation of children complaints is administered out of the CCU office. The position is responsible for conducting complex forensic examinations of digital media that has been involved in computer and internet related criminal activity.

26. What are the minimum education and experience qualifications needed to perform the essential functions of this position.

**EDUCATION:**

Possession of a bachelor's degree with 21 semester (32 term) credits in one or a combination of the following: digital forensics, computer science, information assurance, data processing, computer information, data communications, networking, systems analysis, computer programming, IT project management, or mathematics.

**EXPERIENCE:**

**State Police Digital Forensics Analyst 11**  
No specific type or amount is required.

**KNOWLEDGE, SKILLS, AND ABILITIES:**

- Must understand the importance of the forensic validation process and be thorough while performing forensic examinations.
- Must have considerable working knowledge of computer hardware and software, data networks, LAN's, WAN's, and telecommunications management systems.
- Must have knowledge of performing forensic examinations on digital media.
- Must possess excellent communication skills, both verbal and written.

**CERTIFICATES, LICENSES, REGISTRATIONS:**

None.

*NOTE: Civil Service approval does not constitute agreement with or acceptance of the desired qualifications of this position.*

***I certify that the information presented in this position description provides a complete and accurate depiction of the duties and responsibilities assigned to this position.***

\_\_\_\_\_  
Supervisor

\_\_\_\_\_  
Date

**TO BE FILLED OUT BY APPOINTING AUTHORITY**

Indicate any exceptions or additions to the statements of employee or supervisors.

N/A.

***I certify that the entries on these pages are accurate and complete.***

KELSEY BUCHY

11/4/2022

\_\_\_\_\_  
Appointing Authority

\_\_\_\_\_  
Date

***I certify that the information presented in this position description provides a complete and accurate depiction of the duties and responsibilities assigned to this position.***

\_\_\_\_\_  
Employee

\_\_\_\_\_  
Date