State of Michigan
Civil Service Commission

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

Position Code
1.

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.

2. Employee's Name (Last, First, M.I.)	**8. Department/Agency** STATE POLICE
3. Employee Identification Number	**9. Bureau (Institution, Board, or Commission)** State Services Bureau
4. Civil Service Position Code Description SP DIGITAL FORENSICS ANALYST-A (12)	**10. Division** Intelligence Operations Division
5. Working Title (What the agency calls the position) Digital Forensic Analyst (DFA 12)	**11. Section** Cyber Section
6. Name and Position Code Description of Direct Supervisor Kross, Brian C; STATE POLICE DETECTIVE LT	**12. Unit** Computer Crimes Unit
7. Name and Position Code Description of Second Level Supervisor XXXXXXXXXXX; STATE POLICE FIRST LIEUTENANT	**13. Work Location (City and Address)/Hours of Work** 18050 Deering Street , Livonia, MI 48821 8:00 a.m. to 5:00 p.m. M-F

14. General Summary of Function/Purpose of Position

This position is a regconized resource and responsible for completing forensic examinations of digital media and validation testing of computer hardware and software. This position conducts advanced 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 an advanced 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 advanced 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, including being an expert witness, 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. This position assists the ICAC Task Force Commander manage Internet Cyber Tips involving the exploitation of children. This position maintains servers and systems attached to the Forensic Local Area Network (FLAN) and the Undercover Local Area Network (UCLAN) of the CCU. This position is required to perform all duties in a bias free manner.

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 an advanced 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:

- Generates investigative correspondence consistent with departmental protocol.
- 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 data acquisition and forensic examinations of computers and associated digital media using a variety of approved methods and tools such as: FTK (Imager), X-Ways, Magnet Axiom, Berla, and others.
- Conducts data acquisition and forensic examinations of mobile devices using a variety of approved methods and tools such as: Cellebrite forensic tools, Magnet Software tools, GrayKey, Oxygen Forensic, XRY Forensic, and others.
- 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 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, file systems, Internet browsers, search engines, e-mail systems, databases, and research tools.
- Knowledge of network structures and protocols.
- Knowledge of software applications utilized on computers, mobile devices, and electronic storage devices.
- 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.

Duty 2

General Summary: **Percentage: 10**

Serve as an advanced 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, which may include travel away from the signed office.
- 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, with the ability to be an expert witness, 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.
- Establishes and maintains liaison with Federal, State and Local law enforcement agencies and other entities interested in the training and research in 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:

- Manage and maintain servers and clients connected to the FLAN and the UCLAN.
- Recommend equipment purchases for repairs and upgrades as needed.
- Maintain records of repairs, maintenance, preventative maintenance, upgrades, and modifications to equipment.
- Manage and maintain Software Maintenance and Support (SMS) agreements, renewal schedules, upgrades and modifications to forensic application.
- Assist with designing and installing network cable plants.

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.
- Researches, writes and communicates detailed vendor requests for necessary hardware, software, and equipment according to established guidelines.
- 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**

Manages Internet Cyber Tips involving the exploitation of children. Assists in the prosecution of individuals associated with the illicit use of electronic data storage systems and ensures the preservation of evidence.

Individual tasks related to the duty:

- Assist the ICAC Task Force Commander with the oversight and dissemination of Cyber Tips from the National Center for Missing and Exploited that are assigned to the Michigan ICAC Task Force.
- 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, expert testimony if needed, 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.

Duty 6

General Summary: **Percentage: 5**

Other duties as assigned.

Individual tasks related to the duty:

- Other duties as assigned by supervisors and command staff.

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):

N	Complete and sign service ratings.	N	Assign work.
N	Provide formal written counseling.	N	Approve work.
N	Approve leave requests.	N	Review work.
N	Approve time and attendance.	N	Provide guidance on work methods.
N	Orally reprimand.	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?

Serves as a recognized resource and as an advanced computer forensic specialist and technology crimes investigator, which includes but is not limited to, the potential to lead onsite data captures/investigations and performing forensic analysis. Additional duties include, but are not limited to, replicating media, analyzing logical structures, analyzing data, conducting keyword searches, communication of findings to project managers and clients, working with development to enhance toolsets and processes, and the rendering of testimony in legal proceedings and courts of law. Conducts internet related investigations particularly those involving crimes against children. Processes and analyzes digital mobile devices. All duties listed are essential to the position.

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

Tasks were added to duties 1, 2, and 3. Moved duty #6 to duty #5 and renamed duty #6 to other duties as assigned. Essential functions remain the same. Formatting and spelling corrections.

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 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.

Sp Digital Forensics Analyst-A (12) SPDALTA

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:

Two years of experience equivalent to a State Police Digital Forensics Analyst P11.

Alternate Education and Experience

The education and experience listed below may be substituted for the education requirement.

Educational level typically acquired through the completion of high school and four years of experience equivalent to a database administrator, application programmer, information security analyst, systems administrator, or information technology technician.

OR

Possession of an associate's degree with 16 semester (24 term) credits in digital forensics, computer science, information assurance, data processing, computer information, data communications, networking, systems analysis, computer programming, IT project management, or mathematics and two years of experience equivalent to a database administrator, application programmer, information security analyst, systems administrator, or information technology technician.

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:

For qualification at the 12-level, an individual must be recognized by the International Association of Computer Investigative Specialists as a Certified Forensic Computer Examiner, or possess an equivalent certification from a similar body (this certification is an international industry credential that validates the knowledge of law enforcement and investigative professionals with expertise in forensic examination of computer evidence).

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.

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**