MICHIGAN CIVIL SERVICE COMMISSION

JOB SPECIFICATION

STATE POLICE DIGITAL FORENSICS ANALYST

JOB DESCRIPTION

Employees in this job function as digital forensic professionals performing forensic examinations of digital media and validation testing of computer hardware and software. This includes the coordination and direction of forensic activities on computer-related equipment, networks, and information systems. Investigations may involve any criminal law violation, including the sexual exploitation of children and the possession and distribution of Child Sexually Abusive Materials (CSAM).

There are two classifications in this job.

Position Code Title - Sp Digital Forensics Analyst-E

State Police Digital Forensics Analyst P11

The employee performs a full range of professional assignments. Independent judgment is required to carry out assignments that have significant impact on services or programs. Guidelines may be available, but require adaptation or interpretation to determine appropriate courses of action.

Position Code Title - Sp Digital Forensics Analyst-A

State Police Digital Forensics Analyst 12

This is the advanced level. The employee functions as a senior worker. At this level, employees have regular assignments which have been recognized by Civil Service as having significantly greater complexity than those assigned at the experienced level.

JOB DUTIES

NOTE: The job duties listed are typical examples of the work performed by positions in this job classification. Not all duties assigned to every position are included, nor is it expected that all positions will be assigned every duty.

Reviews requests for complex forensic computer examinations and determines the type and methodology of examination needed.

Conducts forensic examinations of computers and associated digital media.

Conducts data acquisition and forensic examinations of mobile devices using a variety of approved methods and 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.

Assists law enforcement agencies and law enforcement officers in the preparation of affidavits and search warrants.

Works with prosecuting attorneys to ensure proper presentation of digital evidence before and during criminal justice hearings.

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.

Assists with the seizure of computer-related evidence, preparation of search warrants, and the preparation of investigative information for court purposes.

Initiates investigations subsequent to a report of activity involving the illicit use of computer-related systems and associated electronic data storage devices.

Inspects and analyzes computer hard drives and various software packages; decodes passwords and identifies encryptions and data.

Directs and performs investigations involving the use of advanced search programs.

Generates investigative correspondence consistent with departmental protocol.

Conducts vulnerability studies and validation studies on computer hardware, software, and network systems used to conduct computer forensics and cybercrime investigations.

Serves as technical consultant to federal, state, and local law enforcement agencies on computer crime and digital forensic analysis.

Provides expert courtroom testimony for complaints investigated by the Computer Crimes Unit (CCU) and the Internet Crimes Against Children (ICAC) Task Force.

Serves as a member of the ICAC Task Force.

Assists the ICAC Task Force Commander in managing Internet Cyber Tips involving the sexual exploitation of children.

Maintains servers and systems attached to the Forensic Local Area Network (FLAN) and the Undercover Local Area Network (UCLAN) of the CCU.

Assists in the development and implementation of computer forensic training programs for police officers and civilians.

Additional Job Duties

State Police Digital Forensics Analyst 12 (Senior Worker)

Performs, on a regular basis, professional digital forensic assignments, which have been recognized by Civil Service as more complex than those assigned at the experienced level.

JOB QUALIFICATIONS

Knowledge, Skills, and Abilities

NOTE: Considerable knowledge is required at the advanced level.

Knowledge of basic investigative techniques.

Knowledge of theories used in forensic data collection.

Knowledge of operating systems, Internet browsers, search engines, e-mail systems, and research tools.

Knowledge of software applications utilized by suspects during the commission of crimes with digital media, especially CSAM suspects.

Knowledge of forensic tools used in computer forensics.

Knowledge of LAN/WAN/MAN network structures and protocols.

Knowledge of data acquisition methodologies.

Knowledge of the methods and procedures used in a wide variety of e-mail, archiving, and backup systems.

Knowledge of Windows, Apple, and Linux based computer technologies.

Knowledge of the methods and procedures used in the collection and processing of forensic evidence obtained from database, archiving, and back up systems.

Knowledge of design and development of relational databases in support of large-scale digital forensic investigations and data-analysis.

Ability to communicate clearly and concisely both orally and in writing.

Ability to gather and analyze facts, define problems, and devise solutions.

Ability to conduct digital forensics examinations and data-analysis required in the work.

Ability to prepare concise reports detailing findings and conclusions of digital forensic examinations.

Ability to maintain proficiency with industry standard tools and practices.

Ability to maintain a high level of professionalism in all areas of performance.

Ability to provide expert testimony in depositions, trials, and other proceedings.

Ability to multitask and manage several projects at any given time.

Working Conditions

The job requires employees to view graphic material (including images and videos) on a daily basis.

Physical Requirements

The job duties may require an employee to lift and/or move heavy objects.

The job duties may require an employee to stand for extended periods.

The job duties require an employee to possess the agility and coordination to handle equipment and evidence required in the work.

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 P11

No specific type or amount is required.

State Police Digital Forensics Analyst 12

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

Alternate Education and Experience

State Police Digital Forensics Analyst P11 - 12

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 educational level typically acquired through the completion of high school and two years of experience in digital forensics, including the analysis of digital information and physical evidence.

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; 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 one year of experience in digital forensics, including the analysis of digital information and physical evidence.

Special Requirements, Licenses, and Certifications

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). Some positions at the P11 and 12 levels may require other certifications, such as the Certified Electronic Evidence Collection Specialist, EnCase® Certified Examiner, and AccessData Certified Examiner (ACE).

NOTE: Equivalent combinations of education and experience that provide the required knowledge, skills, and abilities will be evaluated on an individual basis.

JOB CODE, POSITION TITLES AND CODES, AND COMPENSATION INFORMATION

Job Code	Job Code Description
STAPOLDIG	STATE POLICE DIGITAL FORENSICS ANALYST

Position Title	Position Code	Pay Schedule
Sp Digital Forensics Analyst-E	SPDALTE	NERE-263
Sp Digital Forensics Analyst-A	SPDALTA	NERE-287

SK

09/13/2015