**New York State Department of Civil Service**
DIVISION OF CLASSIFICATION & COMPENSATION

Classification Standard

***Occ. Code 9213120***

| | |
|---|---|
| **Computer Forensic Analyst 1 (State Police), Grade 14** | **9213120** |
| **Computer Forensic Analyst 2 (State Police), Grade 18** | **9213220** |
| **Computer Forensic Analyst 3 (State Police), Grade 20** | **9213320** |
| **Computer Forensic Analyst 4 (State Police), Grade 23** | **9213420** |
| **Computer Forensic Analyst 5 (State Police), Grade 25** | **9213520** |

Brief Description of Class Series

Computer Forensic Analysts (State Police) are non-competitive, technical positions, performing the full range of analyses of electronic and digital evidence received at the New York State Police Computer Forensic Laboratory and handled by the Computer Crime Unit. Incumbents work as part of a team investigating computer crimes.

These positions are classified only at the Division of State Police and are located at the Computer Forensic Laboratory in Albany.

Distinguishing Characteristics

*Computer Forensic Analyst 1 (State Police):* entry level; conducts data acquisition, tests, and validations of hardware and software; conducts physical examinations of computers and other electronic devices; must successfully complete technical training such as Basic Data Recovery and Acquisition, A+ Hardware, and Network+.

*Computer Forensic Analyst 2 (State Police):* analyzes less complex casework utilizing standard established procedures; must successfully complete technical training such as Intermediate Data Recovery and Analysis, EnCase Computer Forensics I, and Access Data Boot Camp.

*Computer Forensic Analyst 3 (State Police):* analyzes technically complex cases exercising considerable independent judgment; interprets data and results for court purposes; must successfully complete Advanced Data Recovery and Analysis, EnCase Computer Forensics II, and Access Data Windows Forensics.

*Computer Forensic Analyst 4 (State Police):* analyzes the most complex cases, which may involve multiple operating systems and mobile computing devices; must

successfully complete training in multiple operating systems such as Linux, Unix, and MacIntosh, and advanced technical training involving network and wireless devices.

*Computer Forensic Analyst 5 (State Police):* supervisory level; oversees the technical and scientific functions of digital forensics, including supervision of testing procedures and reports of findings; tests analytical methods; oversees training, quality assurance, safety, and proficiency testing; serves as a section head and supervises a unit of Computer Forensic Analysts (State Police).

## Related Classes

Computer Forensic Analysts (Tax) perform the full range of complex analyses of various types of electronic and digital evidence received at the New York State Department of Taxation and Finance. These positions are located in both the Office of Internal Affairs and the Criminal Investigations Division.

State Police Forensic Scientists are non-competitive, technical positions, performing the full range of analyses of various types of evidence received at the State Police Laboratories and handled in either the Drug Chemistry, Biological Sciences, Toxicology, Firearms Examination, or Trace Evidence sections. These positions are in the Forensic Investigation Center in Albany and in the regional Crime Laboratories in New Windsor, Port Crane, and Olean, New York.

## Illustrative Duties

*Computer Forensic Analyst 1 (State Police)*

Follows all procedures related to the proper handling and chain of custody of evidence in computer forensic laboratories.

Uses computer forensic software to forensically copy data found on electronic devices to ensure that the integrity of original evidence is preserved, and the copy can be used for forensic analysis.

Verifies the integrity of the forensic copies used for analysis according to State Police and National Institute of Standards for Technology standards. Uses computer forensics and information technology utilities to verify the integrity of data to ensure that no data is lost or modified during the acquisition or copying process.

Assists with the review of evidentiary data by conducting preliminary research evidence as directed.

Conducts data extractions from electronic devices including mobile phone for evidence preservation.

Performs other laboratory forensic processes following State Police procedures and industry standards and techniques such as secure erase, pursuant to judicial requests or operational requirements.

Conducts physical examinations of computers and other electronic computing devices by inspecting hardware peripherals submitted to the laboratory as evidence. Documents the physical condition of evidence computers and devices by means of digital photography and completion of appropriate examiner reports.

Disassembles and reassembles various types of electronic data or communication devices including but not limited to personal computers, laptops, and cellular phones.

Tests and validates computer hardware, software, and forensic analytical tools using established laboratory procedures and National Institute of Standards for Technology guidelines. Ensures tools do not report high rate of errors.

Prepares and submits required documentation that catalogues and describes acquired data for admittance into evidence in court proceedings.

Reviews and prepares evidentiary material pursuant to Rosario and Discovery court motions such as copying multimedia digital data. May copy multimedia digital data into media to be released to court recognized experts for the purpose of validation, court presentations and possible legal challenges.

Performs computer hardware, software, network, and internet related research to troubleshoot and maintain computer forensic laboratory equipment and network.

Reviews current scientific literature and attends seminars, courses, or professional meetings to stay informed of developments within the field of computer forensics and multimedia digital evidence.

May testify in court proceedings regarding data acquisition, extractions, and evidence handling.

*Computer Forensic Analyst 2 (State Police)*

May perform all the duties of a Computer Forensic Analyst 1 (State Police).

Plans and executes analyses using proper quality control procedures, instrumentation, and techniques.

Examines computers, mobile devices, and other electronic storage devices submitted as evidence using non-intrusive forensic tools and methods to extract data for analysis.

Analyzes data found in electronic devices by using computer forensic utilities and State Police laboratory analytical techniques to parse, locate, and extract case relevant data with evidentiary value pursuant to investigative details and search warrant parameters.

Testifies in court proceedings regarding casework involving routine laboratory processes such as acquisition and analysis.

Prepares comprehensive analysis reports employing State Police report writing standards to be used during investigations, and to be entered into evidence during court proceedings.

Researches industry standards and assists State Police Investigators in developing standard operating procedures for the various stages of computer forensic processes, such as acquisition, archival, and analysis of data.

*Computer Forensic Analyst 3 (State Police)*

May perform all the duties of a Computer Forensic Analyst 1 or 2 (State Police).

Provides technical assistance to State Police Investigators during the extraction of multimedia digital evidence from crime scenes, computer networks, and other technical forensic processes in the field.

Testifies in court proceedings regarding casework involving advanced laboratory processes in difficult cases such as network data acquisitions and advanced data recovery and analysis; and analytical processes and the resulting findings for a wider range of evidence.

Prepares computer and multimedia digital evidence for court presentations under direction from State Police Investigators.

Reviews examinations and analyses completed by other Computer Forensic Analysts and Investigators according to technical peer review guidelines, to ensure that quality assurance standards are met, and those that are deemed to contain nothing of evidentiary value to ensure appropriate forensic steps have been followed.

Recommends changes in standard operating procedures, equipment, and personnel based on results of technical peer review.

Assists in the implementation of hardware and software, as well as modifications to the laboratory equipment and network.

*Computer Forensic Analyst 4 (State Police)*

May perform all the duties of a Computer Forensic Analyst 1, 2, or 3 (State Police).

Analyzes difficult cases based on State Police investigative and forensic procedures and search warrant parameters.

Analyzes the most complex cases, which may involve multiple operating systems and mobile computing devices.

Documents the analysis of laboratory findings in comprehensive reports.

Testifies in court regarding the validity of analyses performed by lower-level Computer Forensic Analysts, the processes used when analyzing digital evidence, and the relation of said evidence to the overall investigation. Testifies in court proceedings regarding difficult cases, which may involve computer networks, multiple operating systems, and mobile computer devices.

Advises State Police Investigators of possible alternative methods of analysis that would increase accuracy, efficiency, and timeliness.

Performs peer review of technically complex cases and reports any unexpected quality control developments that may occur to the lab supervisor.

Assists in training Investigators and Computer Forensic Analysts in the proper acquisition and analysis of digital evidence according to laboratory standard operating procedures.

Administers competency and proficiency tests for all levels of Computer Forensic Analysts to ensure that analysts possess the necessary training and experience to adequately analyze multimedia digital evidence.

*Computer Forensic Analyst 5 (State Police)*

Directs the technical and scientific activities for all forensic analysis in the Computer Forensic Laboratory by establishing unit goals and priorities; managing the workflow of staff; assigning and scheduling staff; evaluating employee performance; overseeing the performance of technical procedures; determining training needs; providing technical guidance; and ensuring staff comply with agency rules, regulations, policies, and procedures.

Reviews reports and examination results from forensic analyses to ensure they meet Computer Forensic Laboratory standards and satisfy the requests of customers.

Coordinates with other New York State Police, federal, county, and local law enforcement agencies on matters involving digital evidence.

Maintains the Computer Forensic Laboratory internal and external training program.

- Provides technical training and lectures to New York State personnel, law enforcement agencies, and other organizations.

- Oversees training, quality assurance, safety, and proficiency testing in the Computer Forensic Laboratory.

Creates and implements Standard Operating Procedures for digital forensic casework.

Performs forensic analyses on difficult cases.

Minimum Qualifications

*Computer Forensic Analyst 1 (State Police)*

Non-Competitive: bachelor's degree in computer forensics, computer science, or a related field; or four years of experience in the field of computer forensics.

*Computer Forensic Analyst 2 (State Police)*

Non-Competitive: bachelor's degree in computer forensics, computer science, or a related field and 18 months of experience as a Computer Forensic Analyst 1 (State Police) or its equivalent in another computer forensic environment.

*Computer Forensic Analyst 3 (State Police)*

Non-Competitive: bachelor's degree in computer forensics, computer science, or a related field and four years of experience performing the duties of a Computer Forensic Analyst 1 (State Police), or its equivalent in another computer forensic environment. Must also possess a computer forensics certification such as EnCE, CFCE, ACE or similar certification. Certification may be substituted with a minimum of 128 hours of computer forensics training; and completion of verifiable training with computer forensic tools such as EnCase, Access Data FTK and ASR SMART.

*Computer Forensic Analyst 4 (State Police)*

Non-Competitive: bachelor's degree in computer forensics, computer science, or a related field and six years of experience performing the duties of a Computer Forensic Analyst 1 (State Police), or its equivalent in another computer forensic environment. Must also possess a computer forensics certification such as EnCE, CFCE, ACE or similar certification; a minimum of 160 hours of verifiable computer forensics training; verifiable training with computer forensics tools such as EnCase, Access Data FTK and ASR SMART; and experience testifying before a court of law or administrative hearing as a computer forensics expert.

*Computer Forensic Analyst 5 (State Police)*

Non-Competitive: bachelor’s degree in computer forensics, computer science, or a related field and seven years of experience performing the duties of a Computer Forensic Analyst 1 (State Police), or its equivalent in another computer forensic environment. Must also possess a computer forensics certification such as EnCE, CFCE, ACE or similar certification; a minimum of 160 hours of verifiable computer forensics training; verifiable training with computer forensics tools such as EnCase, Access Data FTK and ASR SMART; and experience testifying before a court of law or administrative hearing as a computer forensics expert.

Substitution: four years of computer forensic experience may substitute for the bachelor’s degree. A master’s degree in digital forensics or a related field may substitute for one year of experience in computer forensics for all levels in the series.

**Note**: Classification Standards illustrate the nature, extent, and scope of duties and responsibilities of the classes they describe. Standards cannot and do not include all the work that might be appropriately performed by a class. The minimum qualifications above are those required for appointment at the time the Classification Standard was written. Please contact the Division of Staffing Services for current information on minimum requirements for appointment or examination.

11/2022

LEM