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

Classification Standard

Occ. Code 9213110

Computer Forensic Analyst 1 (Tax), Grade 14	**9213110**
Computer Forensic Analyst 2 (Tax), Grade 18	**9213210**
Computer Forensic Analyst 3 (Tax), Grade 20	**9213310**
Computer Forensic Analyst 4 (Tax), Grade 23	**9213410**

Brief Description of Class Series

Computer Forensic Analysts (Tax) are non-competitive, technical positions, performing 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 in the Office of Internal Affairs, and the Criminal Investigations Division, Computer Forensics Laboratory located in Albany, New York.

Distinguishing Characteristics

Incumbents at all levels work as part of teams dedicated to the investigation of computer crimes. They are expected to perform the duties of the lower-level titles in the series, as well as those specific to their title. Incumbents are supervised by an appropriate level manager who, acting as the supervisor for computer forensics and data analytics, assigns cases and sets up work teams based on schedules, staff expertise, and workload. Department Investigators act as team leaders and provide overall coordination of the work that is performed in assigned cases. Generally, incumbents perform their tasks with relative independence, but there are procedural guidelines related to forensic analysis and chain of custody that must be followed for the information to be used as evidence in a court of law.

Computer Forensic Analyst 1 (Tax): entry-level; conducts data acquisition and archival, hardware, software, and tool testing and validation, and physical examinations of computers, electronic devices, and various Department computer network systems; must successfully complete technical training such as Basic Data Recovery and Acquisition, A+ Hardware, and Network+.

Computer Forensic Analyst 2 (Tax): analyzes less complex casework utilizing standard established procedures; may testify in court and other proceedings regarding casework that involves routine laboratory processes such as acquisition, archival, and analysis; plans and executes analyses including proper quality control procedures, using instrumentation and techniques as necessary, and maintaining the proper chain of custody and meeting evidence handling requirements; 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 (Tax): analyzes technically complex cases exercising considerable independent judgment; interprets data and results for court and other adjudicatory purposes; may testify in court and other adverse proceedings regarding casework that involves advanced laboratory processes in complex cases that may include network data acquisitions and advanced data recovery and analysis; must successfully complete technical training such as Intella Basics, Encase Certified Examiner, and Magnet Certified Forensics Examiner while obtaining and maintaining necessary industry-related certifications.

Computer Forensic Analyst 4 (Tax): analyzes the most complex cases, which may involve multiple operating systems and mobile computing devices; testifies in court and other proceedings regarding casework that involves complex networks, 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, while obtaining and maintaining necessary industry-related certifications such as the Certified Computer Forensics Examiner, Certified Computer Examiner, GIAC Certified Forensic Examiner or GIAC Certified Computer Analyst.

Related Classes

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 located only in the Division of State Police and are located at the Forensic Investigation Center in Albany.

Illustrative Duties

Computer Forensic Analyst 1 (Tax): follows all procedures relating to the proper handling and chain of custody of evidence in computer forensic laboratories; uses computer forensic software and robotic tools to forensically copy data found on electronic devices, so that the integrity of original evidence is preserved and the copy can be used for forensic analysis; verifies the integrity of the forensic copies to be used for analysis according to Department and National Institute of Standards for Technology guidelines, 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; uses automated technology to prepare copied data for archiving into digital media and ensures the archival process will preserve and prevent data loss by providing a stable long-term storage medium; conducts physical examinations of computer and other electronic computing devices by inspecting the hardware peripherals in devices submitted to the laboratory as evidence, ensures inspection will encompass device functionality, including date and time verification of circuit board of computer or devices, and 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 during the examination process; tests and validates computer hardware, software, and forensic analytical tools using established Department laboratory procedures and National Institute of Standards for Technology guidelines, and ensures the testing and validation conducted verify the integrity of computer forensic software, data acquisition, and archival hardware and ensures tools do not report high rate of errors; prepares and submits to supervisors any required documentation that catalogues and describes acquired data for admittance into evidence in court proceedings, and submits reports after performing laboratory processes such as acquisition, archival, and analysis; performs computer hardware, software, network, and internet related research to troubleshoot and maintain computer forensic laboratory equipment and network; and reviews current scientific literature, and attends seminars, courses, or professional meetings to stay abreast of developments within the field of Computer Forensics and Multimedia Digital Evidence.

Computer Forensic Analyst 2 (Tax): examines computers 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 Department laboratory analytical techniques to parse, locate, and extract case relevant data with evidentiary value pursuant to investigative details and search warrant parameters; may testify in court and other adverse proceedings regarding casework involving routine laboratory processes such as acquisition, archival, and analysis; uses report writing standards, and prepares comprehensive reports of analyses to be used in the course of investigations, and to be entered into evidence during court proceedings; researches industry standards and assists Department Investigators in developing standard operating procedures for the various stages of computer forensic processes, such as acquisition, archival, and analysis of data; and performs other laboratory forensic processes using Department procedures and industry standards and techniques such as secure erase and hard drive restoration pursuant to judicial requests such as court orders.

Computer Forensic Analyst 3 (Tax): provides technical assistance to Department Investigators during the extraction of multimedia digital evidence from computers, phones, point of sales equipment, computer networks, and other technical forensic processes both in the field and in the lab; testifies in court and other adverse proceedings regarding casework involving advanced laboratory processes in complex cases such as network data acquisitions and advanced data recovery and analysis; under the guidance of Department Investigators in the laboratory and prosecutors, prepares computer and multimedia digital evidence for court presentations, which includes the review of case relevant data and conversion into human readable format that may be displayed during court proceedings, whether in digital form or in printable form; assists Department Investigators in the review and preparation of evidentiary material pursuant to Rosario and other Discovery court motions, which may include the copying of multimedia digital data into media to be released to court recognized experts for the purpose of validation, court presentations, and possible legal challenges; testifies in court regarding analytical processes and findings for a wide range of evidence; recommends changes in standard operating procedures, equipment, and personnel based on results of technical peer review; and assists with the implementation of hardware and software, as well as modifications to the laboratory equipment and network as requested by management.

Computer Forensic Analyst 4 (Tax): analyzes complex cases based on investigative and forensic procedures, and search warrant parameters; documents laboratory findings and analyses in comprehensive reports; testifies in court or other adverse proceedings regarding the validity of analysis performed by lower-level Computer Forensic Analysts, the processes used when analyzing digital evidence, and the relation of evidence to the overall investigation; advises Department Investigators of possible alternative methods of analysis that would increase accuracy, efficiency, and timeliness; reviews the examinations and analyses completed by other Computer Forensic Analysts according to technical peer review guidelines to ensure that quality assurance standards are being met; performs peer review of technically complex cases and reports any unexpected quality control developments that may occur to the lab supervisor; analyzes the most complex cases, which may involve multiple operating systems and mobile computing devices; testifies in court and other adverse proceedings regarding casework in complex cases, which may involve computer networks, multiple operating systems, and mobile computing devices; and administers competency and proficiency tests for lower-level Computer Forensic Analysts (Tax) to ensure that analysts possess the necessary training and experience to adequately analyze multimedia digital evidence.

Minimum Qualifications

Computer Forensic Analyst 1 (Tax)

Non-Competitive: bachelor’s degree in Computer Forensics, Computer Science, or a related field.

Substitution: four years of experience in the field of computer forensics.

Computer Forensic Analyst 2 (Tax)

Non-Competitive: Bachelor’s degree in Computer Forensics, Computer Science, or a related field and two years of experience performing the duties of a Computer Forensic Analyst 1 (Tax) or its equivalent in another computer forensic environment.

Substitution: four years of experience in the field of computer forensics may be substituted for the required bachelor's degree.

Computer Forensic Analyst 3 (Tax)

Non-Competitive: bachelor’s degree in Computer Forensics, Computer Science, or a related field and two years of satisfactory experience performing the duties of a Computer Forensic Analyst 2 (Tax) or its equivalent in another computer forensic environment; and possession of a computer forensics certification such as EnCE, CFCE, ACE, or similar certification.

Substitution: four years of experience in the field of computer forensics may be substituted for the required bachelor's degree. The certification may be substituted with a minimum of 128 hours of computer forensics training or training in a related field, and completion of verifiable training with computer forensic tools such as Encase, Access Data FTK, or Cellebrite. A graduate degree or graduate level courses in Computer Forensics, Computer Science, or related field may substitute for a portion of the 128 hours of computer forensics training, as determined by the credit hours of the program (e.g., a master’s degree with 30 credits may substitute for 30 training hours).

Computer Forensic Analyst 4 (Tax)

Non-Competitive: bachelor’s degree in Computer Forensics, Computer Science, or a related field; two years of experience performing the duties of a Computer Forensic Analyst 3 (Tax) or its equivalent in another computer forensic environment that must also include significant computer forensics casework experience and experience testifying before a court of law or administrative hearing as a computer forensics expert; possession of a computer forensics certification such as EnCE, CFCE, ACE or similar certification; a minimum of 160 hours of verifiable computer forensics training or a professional certification such as the Certified Computer Forensics Examiner, Certified Computer Examiner, Global Information Assurance Certification (GIAC) Certified Forensic Examiner or GIAC Certified Computer Analyst; and verifiable training with computer forensics tools such as Encase, Access Data FTK, and ASR SMART. Candidates must be able to obtain and maintain a professional certification such as the Certified Computer Forensics Examiner, Certified Computer Examiner, GIAC Certified Forensic Examiner, or GIAC Certified Computer Analyst within one year of appointment to this level.

Substitution: four years of experience in the field of computer forensics may be substituted for the required bachelor's degree.

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.

06/2022

KMR