City of Portland

CLASS SPECIFICATION

DIGITAL FORENSICS EXAMINER

PAY GRADE: GRDN0056-P1
CLASS CODE: 30003776
EFFECTIVE: July 20, 2022

CLASSIFICATION SUMMARY

Reports to a Supervisor, Manager, or other supervisory level- position. Under limited supervision, provides specialized forensic computer and digital device examinations and evaluations.

Responsibilities include: analyzing and interpreting computer-based evidence such as email, accounting data, various database extracts, geolocation data, and other information stored on electronic devices; assisting investigators with the proper seizure of computers, cellular devices, storage medium, peripherals, and/or other items functionally reliant upon computer components; supports investigators in digital forensics for cases and provides testimony at trial.

DISTINGUISHING CHARACTERISTICS

Digital Forensics Examiner is a distinct classification.

Digital Forensics Examiner is distinguished from the Crime Analyst series in that the former is responsible for specialized digital forensics analysis and investigations and the latter is responsible for providing case specific crime analysis support.

ESSENTIAL FUNCTIONS

Depending on the assignment, the incumbent may perform a combination of some or all of the following duties, and perform related duties as assigned.

General Duties:

1. Examines and performs comprehensive technical analyses of digital evidence including but not limited to media storage devices, hard drives, network drives, cell phones, and video and still cameras.
2. Takes custody of seized items following accepted evidentiary procedures and policies for the storage of computers or computer related items or components and cellular devices; maintains proper chain of custody.
3. Assists investigators, pursuant to a search warrant or consent, with the proper seizure of computers, storage medium, peripherals, and other items functionally reliant upon computer components such as cell phones, video and still cameras, and other items utilizing microprocessor(s) and/or with data storage capability in an accepted technical manner that ensures preservation of or prevents the destruction of potential evidence.
4. Provides ongoing analysis of technology trends to incorporate proven forensic investigation and supporting technologies into best practice; provides training and consultation on proper seizure and preservation of digital evidence.
5. Provides analytical support for investigators to include social media research, data mining, cell-site mapping, and geo-location of various devices and technologies; creates analytical reports, charts, timelines, and researches new technology to support investigations.

6. Provide technical guidance and assistance in field investigations to ensure data and equipment are preserved; support examination and investigation techniques for other law enforcement and legal entities.
7. Serve as subject matter expert on technical matters relating to digital evidence; make determinations and recommendations regarding appropriate items to be seized based on search warrant particulars and relevant case law; testify in court or at hearings as an expert witness.
8. Collect, preserve, label, catalog, and store evidentiary items for presentation in criminal proceedings in accordance with legal standards and best practices; prepare for defense interviews and trials; compile relevant digital case evidence into a variety of reports; present digital evidence extraction and analysis to investigators.

SUPERVISION RECEIVED AND EXERCISED

The work of this classification is performed under general supervision by a Supervisor, Manager, or other supervisory-level position.

This classification has no supervisory responsibilities.

KNOWLEDGE/SKILLS/ABILITIES REQUIRED

1. Knowledge of principles, practices, and methods of and techniques of digital forensics, current developments, trends, and technologies within the digital forensics field.
2. Knowledge of principles, practices, methods and techniques of investigation.
3. Knowledge of computer operating systems, hardware, software and other peripherals, standard office software, computer forensics software, and presentation software.
4. Knowledge of relevant policies, procedures, administrative rules, laws, regulations, and court decisions.
5. Knowledge of principles, tools, and techniques for project planning and management, and sound business communication.
6. Ability to analyze and evaluate alternatives; provide sound, logical, fact-based conclusions and recommendations.
7. Ability to collect, evaluate, and interpret complex data in statistical and narrative forms.
8. Ability to analyze, interpret, explain, and apply relevant digital forensics laws, regulations, ordinances, policies, and procedures.
9. Ability to communicate clearly, logically, and persuasively, both verbally and in writing; prepare clear, concise, and comprehensive reports, correspondence, and other documents; communicate complex analytical topics to non-technical audiences.
10. Ability to exercise independent judgment, problem-solve, and take initiative within established procedures and guidelines.
11. Ability to establish and maintain effective working relationships with Bureau/Office management and staff, representatives of other public agencies, the public, and others encountered in the course of work.
12. Ability to exercise discretion in confidential and sensitive matters.
13. Ability to maintain accurate files, records, and documentation.
14. Ability to utilize City-specific technology and general office software.

MINIMUM QUALIFICATIONS REQUIRED

Any combination of education and experience that is equivalent to the following minimum qualifications is acceptable.

Education/Training: Bachelor's degree with major coursework in computer science, data process, or a related field;

AND

Experience: Two (2) years of responsible experience in law enforcement, digital forensics, crime analysis, or a related field.

Special Requirements and/or Qualifications:

Ability to pass a police background check.

Law Enforcement Data System (LEDS) and National Crime Information Center (NCIC) certified within 6 months of hire.

A valid state driver's license may be required for certain positions.

Preferred Qualifications:

IACIS Certified Forensic Computer Examiner, SANS GIAC Certified Forensic Examiner, SANS GIAC Advanced Smartphone Forensics, Cellbrite Certified Mobile Examiner

Bargaining Unit: Non-represented
FLSA Status: Non-Exempt
HISTORY
Revision Dates:
9-15-2022: FLSA status changed from Exempt to Non-Exempt