LOS ANGELES UNIFIED SCHOOL DISTRICT
PERSONNEL COMMISSION

CLASS DESCRIPTION
Class Code 1375
Confidential

DIGITAL FORENSIC INVESTIGATOR

DEFINITION

Conducts specialized digital forensic investigations by analyzing hardware and software for digital evidence, prepares evidentiary reports of findings; and as needed, testifies as to findings.

TYPICAL DUTIES

- Conducts digital forensic investigations and scientific analysis of digital evidence to assist District investigators and/or management on student safety issues, fraud, collusion, and/or conflicts of interest.
- Prepares technical reports detailing the evidence retrieval process and comprehensive final forensic reports detailing the results of the forensic investigation for investigators, prosecutors, and/or management.
- Maintains a digital laboratory and assists in updating as necessary.
- Collects and receives digital devices and maintains the chain of evidence by safely storing evidence and documenting the collection and storage of that evidence.
- Disassembles, examines, and identifies computer systems, hardware components, and operational conditions of digital evidence subject to forensic analysis.
- Determines the most appropriate method of protecting original evidence and recovering deleted, erased, hidden and encrypted digital evidence.
- Assists in assembling, configuring, modifying, testing, maintaining, and preparing computers, digital forensics, and network equipment to support the continued operational use of digital devices.
- Dismantles and rebuilds damaged equipment in order to recover lost data as needed.
- Acquires forensic copies (mirror images) of original digital evidence using forensic hardware and software methods.
- Traces URL (Internet) activity, websites visited, history logs, timelines, downloads and manipulations of data.
- Prepares formal materials for presentation in a court of law and testifies as an expert witness.
- Assists investigators and/or management officials by providing technical knowledge and assisting in field investigations.
- Preserves, extracts, analyzes and compiles electronically stored information in response to litigation-related E-discovery requests and Public Records Act (PRA) requests received by the District, in conjunction with the District's PRA Unit and other stakeholders.
- Identifies and recommends computer systems hardware, software, and forensic tools and components to be procured for forensic investigation use.
- Develops and maintains forensic investigation procedures and guides.
- Performs related duties as assigned.

DISTINGUISING CHARACTERISTICS AMONG RELATED CLASSES

A Digital Forensic Investigator performs and may lead specialized computer forensics by performing hardware, software, and virtual analyses of digital evidence and prepares reports, recommendations, and provides expert testimony.

A Forensic Accountant conducts audits of complex financial and operational systems and investigations in relation to alleged improprieties, waste, fraud, and other complaints brought against District departments, employees, vendors, and contractors.

An Electronic Data Analyst conducts complex and sensitive electronic data analysis.

SUPERVISION

General supervision is received from an administrator. Work direction may be exercised over lower-level technical personnel.

CLASS QUALIFICATIONS

Knowledge of:

- Digital devices and associated hardware and peripheral devices
- Electronic data storage, data encryption, and computer security systems
- Methods and principles of forensic data collection and analysis
- Windows, Linux, Unix, MacOS X, DOS, EnCase, Forensic Toolkit (FTK), Nuix, SubRosaSoft, Blackbag Technologies, Helix, AccessData Password Recovery, AccessData Registry Viewer, DNA, Liveview, VMWare, PRTK, Paraben, Datapilot, Cellebrite, Knoppix, Mac Forensic Labs software
- Evidence collection, preservation, and handling
- Software and mobile device technologies, especially as impacts digital forensic activities
- Current technological developments and trends in digital forensics

Ability to:

- Analyze and interpret forensic metadata
- Communicate clearly, concisely, and persuasively orally and in writing to technical and non-technical audiences
- Prepare and present detailed reports and findings
- Find and extract electronically stored information to be used as evidence
- Manage multiple projects expeditiously and maintain precise notes and required documentation
- Establish and maintain effective working relationships
- Recover electronic data that has been deleted, erased, fragmented, hidden, or encrypted from data storage devices
- Stay abreast of current trends and technical advancements in areas of digital forensics
- Maintain confidentiality of investigation records and proceedings
- Keep accurate records
- Gather and recognize salient information and analyze the relationship to matters under investigation

ENTRANCE QUALIFICATIONS

Education:

Graduation from a recognized college or university preferably with a bachelor's degree in computer science, information technology, or a closely related field. Additional qualifying experience may be substituted for the required education on a year-for-year basis, provided that the requirement of a high school diploma or equivalent is met.

Experience:

Two years of experience using current computer forensic hardware, software, and methodologies to conduct digital forensic examinations preferably regarding criminal, civil, serious policy violations and/or child exploitation cases.

Special:

A valid driver's license to legally operate a motor vehicle in the State of California and the use of private transportation, or the ability to utilize an alternative method of transportation.

SPECIAL NOTES

A Certified Forensic Computer Examiner (CFCE), Certified Computer Examiner (CCE), Mobile Forensics Certified Examiner (MCFE) certification or comparable certification must be obtained within the probationary period.

Employees in the class are subject to call at any hour.

The class description is not a complete statement of essential functions, responsibilities, or requirements. Entrance requirements are representative of the minimum level of knowledge, skill, and /or abilities. To the extent permitted by law, management retains the discretion to add or change typical duties of a position at any time, as long as such addition or change is reasonably related to existing duties.

Revised
12-8-2022
SH