CLASSIFICATION NO. 131
Established: 10/13
Revised: 7/16
Revised and Retitled: 12/23
FLSA: Non-Exempt
EEO: 3

DIGITAL FORENSICS ANALYST

CLASS CHARACTERISTICS

Under direction, to conduct advanced and highly specialized computer forensic analyses; to find, identify and extract computerized files and other data of evidentiary value to criminal investigations and the prosecution of crimes; to provide technical guidance and assistance to law enforcement officials involved in investigations; to provide expert testimony in courts regarding electronically stored information; to provide analytical support to investigators; and to do other work as required.

DISTINGUISHING CHARACTERISTICS

The Sheriff's Department provides police protection and law enforcement services to the residents of Clackamas County by enforcing the laws of the State of Oregon. The Department is organized into four major divisions: the Civil Division; Operations Division; Service Division; and Corrections Division.

The Digital Forensics Analyst analyzes and interprets computer-based evidence such as e-mail, accounting data, various database extracts, geolocation data, and other information stored on electronic devices. Incumbents assist investigators, pursuant to a search warrant or consent, with the proper seizure of computers, cellular devices, storage medium, peripherals, and/or other items functionally reliant upon computer components in an accepted technical manner that insures the preservation of or prevents the destruction of potential evidence.

The Digital Forensics Analyst differs from the Detective and the Evidence Technician classifications which are sworn positions responsible for performing complex or specialized criminal investigative work. It also differs from Sergeant which acts as a functional supervisor/lead worker for a team of law enforcement officers.

TYPICAL TASKS

Duties may include but are not limited to the following:

1. Examines and performs comprehensive forensic analyses of computer-related evidence including but not limited to digital data storage devices, external hard drives, network drives, cloud files, smart phones, tablets, 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 related 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 smart phones, tablets, video and still cameras, and other items utilizing a microprocessor(s) and/or with data storage capability in an accepted technical manner that insures the preservation of or prevents the destruction of potential evidence.

4. Conducts training for police personnel on the preservation of electronically stored information; provides information about changes in techniques, technology, and crime scene investigation as it relates to computer forensics.

5. Provides ongoing analysis of technology trends to incorporate proven forensic investigation and supporting technologies into practice; attends periodic training to maintain competency and remain current with evolving technologies.

6. Provides expert testimony in a courtroom setting as required.

7. 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; researches new technology to support investigations; performs other analytical functions as needed.

REQUIRED KNOWLEDGE AND SKILLS

Thorough knowledge of: Principles, methods, and procedures of characteristics of a wide variety of microcomputer systems, including the characteristics of computer equipment, internal computer processes, operating systems, application software, utility programs and magnetic media storage devices; information systems security; network architecture; general database concepts; document management; hardware and software troubleshooting; electronic mail systems; Microsoft Office applications; Apple operating system applications; intrusion tools and computer forensic methodologies, protocols, and tools; methods of security assessments, penetration testing, and ethical hacking; evidence collection, preservation and chain of custody rules/laws.

Skill to: Establish and maintain effective working relationships and credibility with law enforcement officials Deputy District Attorneys, Judges, court staff, outside agencies and the public; dismantle, according to manufactures guidelines and procedures, the components and sub-components of a computer or computer related items and cellular phones, as necessary for a forensic examination; recover electronic data that has been deleted, erased, fragmented, hidden or encrypted from data storage devices; analyze data and information retrieved in the course of duties as it relates to a specific investigation or crime; evaluate and maintain hardware and software necessary for the performance of computer related investigations; conduct security assessments; manage multiple tasks and competing priorities; handle confidentiality appropriately; analyze data and prepare clear, accurate, and comprehensive written and oral reports; follow oral and written instructions; follow Sheriff's Office directives, regulations, procedures, and operations; testify in court; take proper safety precautions, anticipate unsafe circumstances, and act accordingly to prevent accidents; communicate effectively, both orally and in writing.

WORKING CONDITIONS

Duties are typically performed indoors, involving sedentary activities. The Digital Forensic Analyst must understand that through their examinations they will be exposed to viewing emotionally disturbing visual and audible images such as, but not limited to, explicit sex or the sexual or physical abuse of children.

Must be willing to work evenings and weekends as required. Requires on-call availability beyond assigned shifts.

MINIMUM QUALIFICATIONS

Minimum qualifications are used as a guide for establishing the minimum experience, education, licensure, and/or certifications required for employment in the classification. The following minimum qualifications are established for this classification. Additional minimum qualifications and special conditions may apply to a specific position within this classification and will be stated on the job announcement.

Experience: A minimum of three (3) years of related experience that would provide the required knowledge and skills to perform the responsibilities of this position.

Licenses/Certifications: None Required.

PRE-EMPLOYMENT REQUIREMENTS

Positions within the County's Criminal Justice agencies must successfully pass an extensive background investigation which may include national fingerprint records check.

All positions within the County's Criminal Justice agencies must pass a pre-employment drug test.

Driving is required for County business on a regular basis or to accomplish work. Incumbents must possess a valid driver's license, and possess and maintain an acceptable driving record throughout the course of employment.