DIGITAL FORENSIC INVESTIGATOR

JOB PURPOSE AND SUMMARY

The Computer Forensic Investigator is assigned to the Investigative branch of the Clark County Sheriff's Office and is expected to facilitate the work of the different investigative units and the Prosecuting Attorney's Office. Investigations are expected to be accomplished by applying specialized knowledge and skills to conduct highly technical analyses and procedures in the collection, processing, preservation and presentation of digital evidence to assist law enforcement in a variety of criminal investigations; act as a technical expert regarding police computer forensics; prepare detailed reports of investigations and analysis; assist prosecuting attorneys with trial preparation to coordinate digital evidence presentation; make court appearances and give testimony relating to cases; deploy into the field to assist in locating digital evidence at crime scenes, and support search warrant services.

This is a full-time, regular, non-exempt position that will have a limited law enforcement commission.

KEY OR TYPICAL TASKS AND RESPONSIBILITIES

- Conduct seizures and examinations of electronic devices including cell phones/smart phones, tablets, laptops, personal computers and corresponding electronic data storage media to secure and recover data as evidence; Assist in the execution of search warrants for evidence in criminal investigations. Conduct on-site forensic analysis previews of digital evidence. Act as subject matter expert: make determinations and recommendations regarding appropriate items to be seized based on search warrant particulars and relevant case law.

- Assist Detectives and multi-jurisdictional law enforcement agencies in legal preparation and authoring of search warrants and subpoenas to properly obtain subscriber records and seizure of all types of electronic devices media as evidence. Additionally, ESP/ISP subscriber records and content.

- Assist detectives and other law enforcement agencies with criminal investigation that have a digital component, including persons crimes such as murder, rape and robbery; child sexual exploitation crimes such as child sexual abuse depictions and/or materials, child abuse and child sex trafficking; cyberstalking and domestic violence related crimes and department investigations of its members that include a non-criminal administrative computer forensic need.

- 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. Put together all relevant digital case evidence in easy-to-understand format. Present the digital evidence extraction and analysis to prosecutors and defense teams for pre-trial defense interviews. Present digital evidence in trial and respond to questions regarding findings.

- Compose reports on findings from digital evidence extraction and analysis.

- Keep knowledgeable of changes in local, state, and federal laws and best practices. Provide recommendations for changes to departmental policy or procedure and the recommendation for purchase of equipment as it relates to digital forensics.

- Perform other duties and responsibilities as assigned.

EXPERIENCE AND EDUCATION

United States Citizenship or Lawful Permanent Resident required.

Education: Associate's Degree in an Information Technology related field. Equivalent combinations of education and experience may be considered.

Experience: Two (2) years of increasingly responsible experience in digital evidence analysis, preferably in a law enforcement environment.

Computer skills: Intermediate skills utilizing two or more of the following platforms used for digital forensics analysis: EnCase, Cellebrite, X-Ways, Axiom, Griffeye, Recon and AccessData FTK. Intermediate skills in Microsoft Word, Excel, Outlook, PowerPoint.

Required Licenses and/or Certifications: At least one industry accepted certification directly related to digital forensics, such as IACIS, Cellebrite, EnCase (EnCE), SCERS, or other industry accepted certification(s) directly related to digital forensics.

Knowledge of: principles, methods and practices of investigation; evidence identification and collection; PC and MAC operating systems, hardware, and other peripherals; rules of evidence and applicable laws is critical; fundamental principles and procedures of record keeping; English usage, spelling, grammar and punctuation; comprehensive knowledge of computer forensic software; pertinent federal, state and local laws that pertain to: collection, processing, and preservation of computer related evidence; modern office procedures, methods and computer equipment; use of personal computers and basic software.

Ability to: collect, preserve, label, catalog, and store evidentiary items for presentation in criminal proceedings in accordance with legal standards; utilize computer hardware and software and other equipment commonly used in analysis and recovery of computer data; learn to interpret and apply Federal, State, and local policies, procedures, laws and regulations; work independently with minimal supervision; maintain confidentiality related to the area of work; operate and use modern office equipment including a personal computer and appropriate computer programs; communicate clearly and concisely, both orally and in writing; operate a personal computer and appropriate software; work and act as a team player in all interactions with other employees; provide a high level of customer service at all times; project and maintain a positive image with those contacted during work; develop and maintain collaborative and respectful working relationships with team members and others; consistently provide quality service; maintain regular and dependable attendance.

Revised: 01/18/2022 (Civil Service only)
Created: 12/15/2020