UTAH COUNTY JOB DESCRIPTION

CLASS TITLE: FORENSIC COMPUTER ANALYST I, II, III
CLASS CODE: I – 3491 II – 3492 III – 3493

FLSA STATUS: NON-EXEMPT
SUPERVISORY STATUS: FORENSIC COMPUTER ANALYST I, II - NONE
FORENSIC COMPUTER ANALYST III - LEAD

EFFECTIVE DATE: 09/13/2016
DEPARTMENT: SHERIFF

JOB SUMMARY
Under general supervision from the Evidence Crime Lab Supervisor, collect, preserve, and analyze digital and electronic evidence through the use of specialized investigative tools in both criminal and internal investigations. This civilian position is part of the Utah Retirement System for Public Employees

CLASS CHARACTERISTICS
Forensic Computer Analyst I: This is the entry and training classification for analysts possessing a B.A. or B.S. degree or qualifying experience.
Forensic Computer Analyst II: This is the full performance classification of the series responsible to perform assignments with minimal supervision and guidance and possesses level II certifications.
Forensic Computer Analyst III: This lead classification requires the ability to provide guidance/direction to peace officers, evidence technicians and computer analysts.

ESSENTIAL FUNCTIONS
- Collect, preserve, examine, analyze, and process digital evidence using specialized investigative tools and without altering original evidence.
- Recover digital evidence in deleted, hidden, encrypted, corrupted, and protected electronic files in order to expose and recover digital evidence.
- Develop, update, and implement procedures relating to the seizure and examination of evidence from computer and other digital media.
- Prepare detailed and comprehensive reports of findings for submission to law enforcement.
- Partner with law enforcement to execute off-site search warrants by triage, seizing, imaging, and analyzing computer and digital devices pertinent to investigations.
- Serve as technical expert and consultant with law enforcement agencies conducting internal or criminal investigations involving computer and digital evidence.
- Prepare and submit grant proposals in a timely manner, monitor grant fiscal and performance compliance, submit required reports to comply with and maintain grant funding.
- Acquire, install, and maintain all hardware and software necessary to effectively conduct forensic science activities related to digital evidence.
- Research and implement forensic analysis best practices, emerging technologies, and strategies.
- Receive, maintain, and release evidence in accordance with evidence-handling procedures and best practices.

- Testify in court or before administrative bodies as a technical expert and expert witness as to the procedure and method used to collect, preserve, inventory, examine, and analyze digital evidence and the results of analyses conducted.
- Provide pertinent training to law enforcement personnel and agencies.
- Acquire and maintain all certifications and credentials applicable to job function and duties.
- Partner with state, county, and city law enforcement agencies with high profile or complex cases as requested.
- Provide expert assistance to detectives and other law enforcement personnel related to the documentation and processing of crime scenes and the collection and preservation of evidence.
- Perform all duties of the evidence custodians and technicians, as necessary, to efficiently carry out department operations.
- Prepare and participate in court proceedings; determine completeness of information, adequacy of evidence and general preparedness of various cases for prosecution; present testimony in court relevant to cases investigated; assist prosecutors in preparing exhibits, evidence, and witnesses for court.

KNOWLEDGE, SKILLS, AND ABILITIES

Knowledge: Maintain current knowledge of federal and state statutes and recent appellate case rulings pertaining to digital crimes and evidence; advanced working knowledge of Windows, OSX, and Linux Operating Systems and their accompanying file systems; advanced working knowledge of computer networks, network components, network security, and network setup.
Skills: Verbal and written communication; compose technically-complex information in an easy-to-understand format; work with peace officers and attorneys effectively and professionally; analyze complex digital systems and data, including systems/data protected by passwords or other means designed to prevent examination/analysis; design, install, and maintain computer hardware and software for a digital forensic evidence laboratory.
Abilities: Work with minimal supervision; communicate effectively (verbal and written) learn new technology (hardware and software); for forensic analysis; meet timely deadlines and reach goals; troubleshoot computer hardware and software problems; research and implement emerging technologies; attend training to maintain a high degree of proficiency to meet current demands. Work cooperatively in a team environment.

PHYSICAL DEMANDS

Frequently: Work for sustained periods of time and maintain concentrated attention to detail.
Regularly: Sits, walks, stands, stoops, kneels, crawls or crouches; encounters strong smells; uses arms to reach out and above head; drives a motor vehicle; distinguishes between shades of color.
Occasionally: Lift or otherwise move objects weighing up to 50 pounds.

Accommodation may be made for some of these physical demands for otherwise qualified individuals who require and request such accommodation.

WORKING CONDITIONS

Work is typically performed in an environmentally controlled building, but is regularly performed off-site, in a variety of settings. Work is occasionally performed for sustained periods outdoors including in hot, cold, or

inclement weather. Work requires some traveling and transporting of equipment to off-site locations by vehicle. Work occasionally exposes incumbent to high levels of noise, contagious or infectious diseases, bodily fluids and/or hazardous chemicals. Work occasionally requires the use of protective devices such as personal body armor, masks, goggles, and gloves. Work exposes incumbent to possible bodily injury from working on or transporting equipment, tools, or machinery or from potentially hostile situations and to unknown and dangerous situations.

EDUCATION AND EXPERIENCE

Forensic Computer Analyst I: Bachelor's degree from an accredited university in computer engineering, computer science, computer information systems or a closely-related field OR five years' work experience as a forensic computer analyst, investigating and performing crime lab duties, conducting criminal investigations, or processing evidence in a field-related environment.
Forensic Computer Analyst II: Bachelor's degree from an accredited university and four years of work experience as a forensic computer analyst OR five years' experience as a computer forensic analyst and an additional five years' experience as a certified law enforcement officer, conducting criminal investigations and processing crime scenes.
Forensic Computer Analyst III: Bachelor's degree from an accredited university and six years of work experience as a forensic computer analyst OR seven years' experience as a computer forensic analyst and an additional five years' experience as a certified law enforcement officer, conducting criminal investigations and processing crime scenes.

A master's degree in a related field may substitute for one year of work experience and a doctorate in a related field for three years of work experience.

Preference may be given to retired law-enforcement officers

LICENSING AND CERTIFICATION

- Offer contingent upon the successful completion of a safety-sensitive background check.
- Applicant must possess a current driver's license and obtain a valid State of Utah driver's license within 60 days of employment.

Forensic Computer Analyst I: Must obtain the following certifications within one year of starting employment with Utah County:

- Basic Computer Evidence Recovery Training (BCERT) through the U.S. Secret Service National Computer Forensics Institute;
- Certified Forensic Computer Examiner (CFCE) through International Association of Computer Investigative Specialists (IACIS); AND
- EnCase® Certified Examiner (EnCE®) through Guidance Software (AccessData Certified Examiner (ACE) through AccessData may be substituted at this level).

Forensic Computer Analyst II: Must possess certifications of level I and obtain the following certifications during the first year of hire or promotion for County employees promoted to this classification through a competitive recruitment process:

- Advanced Forensic Training (AFT) through the U.S. Secret Service National Computer Forensics Institute; AND
- EnCase® Certified Examiner (EnCE®) through Guidance Software (AccessData Certified Examiner (ACE) through AccessData may be substituted if ENCase was previously obtained).

County employees being reassigned, transferred, or promoted through career ladder advancement to this classification must possess said certifications and licensure upon reassignment, transfer, or career ladder advancement.

Forensic Computer Analyst III: Must possess certifications of level I and II and obtain the following certifications during the first year of hire or promotion for County employees promoted to this classification through a competitive recruitment process:

- Network Intrusion Responder Program (NITRO) through the U.S. Secret Service National Computer Forensics Institute;
- X-Ways Certified Examiner through X-Ways Software Technology.

County employees being reassigned, transferred, or promoted through career ladder advancement to this classification must possess said certifications and licensure upon reassignment, transfer, or career ladder advancement.

CAREER LADDER ADVANCEMENT

For promotion through career ladder advancement from a lower classification level of this series to a higher one, there must be funding in the budget and the employee must: 1) possess the required licensure and certifications of the higher classification level, 2) meet the education and experience requirements and class characteristics of the higher classification level, 3) have written recommendation from the department head and, 4) receive approval from the Director - Office of Personnel Management.

This description lists the major duties and requirements of the job and is not all-inclusive. Incumbent(s) may be expected to perform job-related duties other than those contained in this document and may be required to have specific job-related knowledge and skills.